



Vulnerability Assessment Framework 1.1

Prepared under contract for the
Critical Infrastructure Assurance Office

by
KPMG Peat Marwick LLP

October 1998



CIAO

Notice: This document was prepared as an account of work sponsored by an agency of the United States Government. Neither the United States Government nor any agency thereof, nor any of their contractors, subcontractors, or their employees, makes any warranty, express or implied, or assumes any legal liability or responsibility for the accuracy, completeness, or usefulness of any information, apparatus, product, or process disclosed, or represents that its use will not infringe on privately owned rights. Reference herein to any commercial product, process, or service by trade name, trademark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by the United States Government, any agency thereof or any of their contractors or subcontractors. The views and opinions expressed herein do not necessarily state or reflect those of the United States Government or any of their contractors.



CIAO

October 1998

Presidential Decision Directive 63 directs every department and agency of the Federal Government to develop a plan by November 18, 1998, to protect its own critical infrastructure, including but not limited to its cyber-based systems. While your department should decide the shape of the plan best suited to your mission, you may wish to consider basing your plan on an identification of your critical infrastructures and their vulnerabilities, including:

- identification of mission essential telecommunications, information, and other systems;
- identification of significant vulnerabilities of the department's minimum essential systems;
- internal and external interdependencies; and
- an assessment of the vulnerability of the department's minimum essential services to failures by private sector providers of telecommunications, electrical power, and other infrastructure services.

The Vulnerability Assessment Framework (VAF) is designed to assist your agency's work on these issues. The VAF was produced by KPMG Peat Marwick LLP, under contract to the Critical Infrastructure Assurance Office, with review and input over the last six weeks from a wide range of agencies. Based on existing security requirements and standards, the VAF can be applied across the federal government as well as to private sector infrastructures.

Through a three-step process, the VAF will enable your organization to define your Minimum Essential Infrastructure (MEI), identify and locate interdependencies and vulnerabilities of your MEI, and provide the basis for developing your remediation plans. The VAF has been designed with inherent scalability so that it is applicable to all levels of government as well as broad sectors of the National infrastructure as well.

Should your department choose to do so, the VAF can be a core component of your agency's plan. Further assistance and guidance on overall agency planning to protect your critical infrastructures will be forthcoming from the General Services Administration and the Critical Infrastructure Assurance Office.

As you prepare your agency's internal plans, and in many cases the sector plans, you will find the VAF to be a useful tool in guiding you to find the vulnerabilities that need remediation so that our Nation's infrastructures are secured. The Critical Infrastructure Assurance Office staff and I stand ready to assist agencies in their planning efforts. For assistance with the VAF, please contact the CIAO at (703) 696-9395.

Sincerely,

Jeffrey A. Hunker
Director





CIAO

(Page Left Intentionally Blank)



TABLE OF CONTENTS

PREFACE.....	1
I. INTRODUCTION.....	4
ROLE OF SENIOR MANAGEMENT.....	5
THE FRAMEWORK.....	6
AUDIENCE.....	7
OBJECTIVES AND CRITICAL SUCCESS FACTORS.....	7
SCALABILITY OF THE FRAMEWORK.....	8
II. THE VAF APPROACH.....	9
III. VAF STEP 1 - ESTABLISH THE MINIMUM ESSENTIAL INFRASTRUCTURE (MEI).....	11
VAF STEP 1.1—IDENTIFY THE CORE MISSION(S) OF THE ORGANIZATION.....	18
VAF STEP 1.2—IDENTIFY THE THREAT ENVIRONMENT.....	19
VAF STEP 1.3—IDENTIFY THE PROCESSES SUPPORTING THE STRATEGIC OR CORE MISSION(S).....	22
VAF STEP 1.4—ANALYZE THE VALUE OF EACH CORE PROCESS.....	23
VAF STEP 1.5—IDENTIFY ORGANIZATIONAL STRUCTURE AND CUSTOMERS.....	25
VAF STEP 1.6—IDENTIFY FACILITIES.....	26
VAF STEP 1.7—MAP CYBER ARCHITECTURE, DATA AND SYSTEMS.....	27
VAF STEP 1.8—LINK PHYSICAL, ORGANIZATIONAL, ARCHITECTURE COMPONENTS TO THE CORE PROCESSES THAT PLAY KEY ROLES IN ACHIEVING THE MISSION.....	29
VAF STEP 1.9—IDENTIFY THE EXTERNAL RESOURCES UPON WHICH THE MEI IS DEPENDENT.....	30
IV. VAF STEP 2 - GATHER DATA TO IDENTIFY MEI VULNERABILITIES.....	32
VAF STEP 2.1—ASSESS AREAS OF CONTROL—ENTITY WIDE SECURITY.....	41
VAF STEP 2.2—ASSESS AREAS OF CONTROL—ACCESS CONTROLS.....	45
VAF STEP 2.3—ASSESS AREAS OF CONTROL—SEGREGATION OF DUTIES.....	53
VAF STEP 2.4—ASSESS AREAS OF CONTROL—CONTINUITY OF SERVICES AND OPERATIONS.....	55
VAF STEP 2.5—ASSESS AREAS OF CONTROL—CHANGE CONTROL & LIFE CYCLE MANAGEMENT.....	59
VAF STEP 2.6—ASSESS AREAS OF CONTROL—SYSTEM SOFTWARE.....	62
V. VAF STEP 3 - ANALYZE & PRIORITIZE VULNERABILITIES.....	64
VAF STEP 3.1—DOCUMENT THE IMPACT.....	66
VAF STEP 3.2—DOCUMENT THE VULNERABILITIES.....	67
VAF STEP 3.3—SUMMARIZE THE VULNERABILITIES.....	68
VAF STEP 3.4—EVALUATE THE VULNERABILITIES.....	69
VI. NEXT STEPS.....	71



CIAO

VII. GLOSSARY OF TERMS.....	72
VIII. PRIMARY SOURCE DOCUMENTS.....	77
APPENDIX A: ENTITY-WIDE SECURITY.....	A-1
ORGANIZATIONAL MANAGEMENT.....	A-1
SECURITY PROGRAM PLAN.....	A-3
SECURITY MANAGEMENT.....	A-4
HUMAN RESOURCES POLICIES.....	A-6
OUTSOURCING.....	A-8
ELECTRONIC COMMERCE.....	A-9
APPENDIX B: ACCESS CONTROLS.....	B-1
DATA TYPES.....	B-1
ACCESS CONTROL LISTS (ACL).....	B-1
PHYSICAL CONTROLS.....	B-4
DATA CENTERS.....	B-36
PHYSICAL ACCESS LISTS AND VISITOR LOGS TO DATA CENTERS.....	B-37
PHYSICAL KEYS, CARD KEYS AND CIPHER LOCKS.....	B-39
PASSWORDS.....	B-42
NETWORK MANAGEMENT SYSTEMS (NMS).....	B-44
SECURITY SOFTWARE.....	B-46
DBMS.....	B-47
REMOTE ACCESS.....	B-48
ENCRYPTION AND RELATED APPLICATIONS.....	B-50
MONITORING.....	B-53
DATASCOPIES AND SNIFFERS.....	B-54
HUB MANAGEMENT.....	B-55
VOICE OPERATIONS.....	B-55
APPENDIX C: SEGREGATION OF DUTIES.....	C-1
POLICIES.....	C-1
ACCESS CONTROLS TO ENFORCE SEGREGATION OF DUTIES.....	C-4
OPERATING PROCEDURES, SUPERVISION, AND REVIEW.....	C-4
APPENDIX D: CONTINUITY OF SERVICE AND OPERATIONS.....	D-1
BUSINESS CONTINUITY PLAN.....	D-1
RESOURCE MANAGEMENT—COB.....	D-5
CONTINGENCY PLAN.....	D-8
SERVICE LEVEL AGREEMENT MANAGEMENT.....	D-10
DATA CENTER MANAGEMENT.....	D-11
BACK-UP MANAGEMENT.....	D-19



CIAO

ALTERNATIVE SITE MANAGEMENT.....	D-21
INTERDEPENDENCY AWARENESS.....	D-22
MONITORING.....	D-22



CIAO

APPENDIX E: CHANGE CONTROL & LIFE CYCLE MANAGEMENT.....	E-1
CHANGE MANAGEMENT.....	E-1
SYSTEM DEVELOPMENT LIFE CYCLE MANAGEMENT.....	E-3
PROJECT MANAGEMENT.....	E-9
APPLICATION ACQUISITION, MANAGEMENT, AND MAINTENANCE.....	E-13
QUALITY AND ASSURANCE.....	E-16
APPENDIX F: SYSTEM SOFTWARE.....	F-1
SYSTEM SOFTWARE ACCESS CONTROL.....	F-1
SYSTEM SOFTWARE MONITORING (ACCESS AND USE).....	F-4
SYSTEM SOFTWARE CHANGE CONTROL.....	F-5
APPENDIX G: WHITE PAPER.....	G-1



CIAO

(Page Left Intentionally Blank)



CIAO

Preface

“A Growing Potential Vulnerability”

“The United States possesses both the world’s strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation’s critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.”

“President’s Intent”

“It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.”

“A National Goal”

“No later than [May 22] the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63, [May 22, 2003], the United States shall have achieved and shall maintain the ability



CIAO

to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States."

"A Public-Private Partnership to Reduce Vulnerability"

"Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector."

"Protecting Federal Government Critical Infrastructures"

"Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.

No later than 180 days, [November 18, 1998], from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. No later than two years from today, [May 22, 2000] those plans shall have been implemented and shall be updated every two years. In meeting this



CIAO

schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure. The Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.”

“Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.”

“Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.”

Excerpts from the
WHITE PAPER
The Clinton Administration’s Policy on
Critical Infrastructure Protection:
Presidential Decision Directive 63
May 22, 1998



I. Introduction

On August 18, 1998, KPMG Peat Marwick LLP commenced the task of creating a Vulnerability Assessment Framework (VAF) under contract to the Critical Infrastructure Assurance Office in response to Presidential Decision Directive (PDD) 63. In assuming this task, KPMG has taken a business approach to developing this vulnerability assessment tool as opposed to a national security approach. The former incorporates established business risk assessment measurements in a holistic approach to assessing physical and cyber vulnerabilities. The latter has historically been primarily driven by the known or suspected capabilities of identified adversaries.

While some suggest that penetration testing is an adequate approach to assessing cyber vulnerabilities, KPMG's experience clearly indicates the need for a more holistic approach. Penetration testing is but one part—and a temporary one at that—to overall vulnerability assessment. Identification of the root causes of vulnerabilities through other assessment criteria enables systemic remedies, not just temporary patches. It was KPMG's intent to propose a VAF that would lead to systematic remedies.

Although there have been historical differences in approach to measuring business risk and assessing threats to national security, the flexibility of the VAF developed by KPMG allows it to be applied in either arena. The difference comes through the level of detail that agencies want to address or national security standards to which the VAF methodology is applied. To the extent it is possible to do so, the VAF may also be applied in the context of requirements of the Computer Security Act of 1987 or other federal requirements.

For purposes of this effort, the approach adopted in the President's Commission on Critical Infrastructure Protection (PCCIP) report regarding threats and vulnerabilities has been utilized. In a world of non-conventional threats, cyber or physical, it is not prudent to suppose that an organization will know in advance from where a threat may arise.

As noted by the PCCIP, the right command sent over a network to a power generating station's control computer could be just as effective as a backpack full of explosives. However in the former scenario, the perpetrator would be harder to identify and apprehend. The rapid growth of a computer-literate population ensures that increasing millions of people possess the skills necessary to consider such an attack. The wide adoption of public protocols for system connectivity and the availability of "hacker tool" libraries make their task easier. While the resources needed to conduct a physical attack have not changed considerably, the resources necessary to conduct a cyber attack are now commonplace. A personal computer and a simple telephone connection to an Internet Service Provider (ISP) anywhere in the world are enough to cause great damage.

The PCCIP further noted that our infrastructures have substantial vulnerabilities to domestic and international threats. For those intrusions that are known, insiders have been primarily at the root



of the exploitation of these vulnerabilities. Because it may be impossible to determine the nature of a threat until after it has materialized, infrastructure owners and operators—most of whom are in the private sector—must focus on protecting themselves against the tools of disruption, while the government helps by collecting and disseminating the latest information about those tools and their employment. The Commission did not discover an immediate threat sufficient to warrant a fear of imminent national crisis. However, vulnerabilities are becoming more common with the introduction of new technologies, the widespread use of electronic media, the inadequate administration of technical and operational controls, the ready availability of means to exploit those weaknesses, and the decreasing costs associated with an effective attack.

Thus, the traditional security approach of monitoring the activities of known or potential attackers or intruders breaks down. The first line of infrastructure defense must now be to identify and resolve vulnerabilities before they are exploited. Protecting our infrastructures into the 21st Century requires that we develop greater understanding of their vulnerabilities and act decisively to reduce them.

Role of Senior Management

In a recently-published study of leading organizations, the U.S. General Accounting Office (GAO) found that senior executive recognition of information security risks and interest in taking steps to understand and manage these risks are the most important factors in prompting development of more formal information security programs. Such high-level interest helps ensure that information security is taken seriously at lower organizational levels and that security specialists have the resources needed to implement an effective program.

The study further noted that business managers, usually referred to as program managers in federal agencies, must bear the primary responsibility for determining the level of protection needed for information resources that support business operations. In this regard, business managers should be held accountable for managing the information security risks associated with their operations, much as they would for any other type of business risk. However, security specialists play a strong educational and advisory role and have the ability to elevate discussions to higher management levels when they believe that risks are not being adequately addressed. Business managers are generally in the best position to determine which of their information resources are the most sensitive and what the business impact of a loss of integrity, confidentiality, or availability would be.

GAO's survey also determined that business or program managers are in the best position to determine how security controls may impair their operations. For this reason, involving them in selecting controls can help ensure that controls are practical and will be implemented. Accordingly, security specialists have assumed the role of educators, advisors, and facilitators who help to ensure that business managers are aware of risks and of control techniques that have



CIAO

been or could be implemented to mitigate the risks. For several of the organizations, these roles represent a dramatic reversal from past years, when security personnel were viewed as rigid, sometimes overly protective enforcers who often did not adequately consider the effect of security controls on business operations.

The PCCIP characterized its infrastructure assurance initiatives as the beginning of a long process, but one that may never be concluded. The organizations in GAO's survey emphasized the importance of continuous attention to security to ensure that controls are appropriate and effective. They stressed that constant vigilance and frequent reassessment are needed to ensure that controls remain appropriate--addressing current risks and not unnecessarily hindering operations--and that individuals who use and maintain information systems comply with organizational policies. Such attention is important for all types of internal controls, but it is especially important for security over computerized information, because, as mentioned previously, the factors that affect cyber security are constantly changing in today's dynamic environment.

The Framework

Numerous reference documents have been identified and reviewed for possible relevance. Upon analysis, and on the basis of actual experience in the assurance/audit arena, the KPMG VAF methodology has drawn heavily from several different current processes for measuring information technology (IT) system controls. These include: the April 1998 Control Objectives for Information Technology (COBIT™) process of the Information Systems Audit and Control Foundation (ISACF); the May 1998 publication "Executive Guide Information Security Management" of the United States General Accounting Office (GAO); and GAO's standards for auditing federal information systems (Federal Information Systems Control Audit Manual (FISCAM)).

Of course, the above approaches above were not designed to fully apply to the issues that surface when attempting to assess infrastructure vulnerabilities. Nonetheless, parts of each of these were considered relevant for several reasons. First, each represents a current approach to system controls used by IT auditors. Second, each has drawn extensively from other sources, some both national and international, resulting in a broader base of expertise in IT governance practices. Third, although suggested for applicability to cyber system controls, at least part of the control standards defined in each document can apply to the physical vulnerabilities as well.

Finally, the KPMG VAF methodology has also drawn from the report of the PCCIP. In particular, the PCCIP findings concerning the issue of interdependencies and their approach to threat and vulnerability issues have been incorporated. PDD 63 instructed that the government and sectoral vulnerability assessment plans include a particular focus on interdependencies. So, it is important to understand what the term "interdependency" means and how it should apply to the



CIAO

vulnerability assessment plans of government departments and agencies. Since PDD 63 specifically states that the VAF “shall include the determination of minimum essential infrastructure” (MEI), it will also be important to understand what it means and how it applies.

If your organization is already performing vulnerability assessments, the team should examine the process being used against the VAF process and determine if gaps between the two exist. The intent of the VAF process is to use, if available, existing data gathering and analysis techniques in the identification and documentation of vulnerabilities in the infrastructure. The intent is not to duplicate existing efforts.

Audience

The initial audience for the VAF template consists of the departments and agencies of the federal government. Additionally, the VAF should be able to address the needs of the private sector, for which the government should be a model. We envision that this plan will be used to assist management in analyzing their Minimum Essential Infrastructure (MEI), its strengths, weaknesses, and external dependencies.

In order to implement the VAF process, a leadership team should be formed. This team will consist of the agency CIAO, CIO, a person familiar with the audit and oversight outputs of the Inspector General and persons responsible for information and data security, physical security, and personnel security. The precise skill sets required are defined in greater detail in section III.F.

In addition to management, the plan is designed to be used by security professionals and internal auditors. It will serve as a common language and facilitate communication, expectations, and cooperation among the three groups. This will aid them in effectively working together as a team, understanding the tasks to be accomplished, and achieving the common goal of minimizing vulnerabilities that may diminish the agency’s ability to achieve its mission or the robustness of the National MEI (e.g. the critical national infrastructures).

Objectives and Critical Success Factors

The objectives and critical success factors of the VAF are as follows:

- The VAF must apply to infrastructure vulnerabilities in both physical and cyber dimensions.
- The VAF must be scalable, capable of being applied by large, sophisticated government organizations, as well as by small government entities with little, or no, experience with infrastructure vulnerability issues.



CIAO

- The VAF must be flexible, allowing the user to give emphasis to those areas of the VAF of greatest importance to the individual agency.
- The VAF should be able to address two audiences: the government agencies that would initially apply it, and the private sector for which the government should be a model.
- The VAF should incorporate a delivery mechanism that is readily acceptable to both government and the business world, and not one that would require new government regulation or structures. (The VAF can be implemented by an auditor, both within the context of business risk assessment, and the growing accountancy requirement to assess risks and adequacy of controls over information technology systems.)
- The VAF must be flexible enough to draw from other sources of expertise for updated analytical information. Just as many of the concepts of this VAF are drawn from COBIT™, GAO, OMB, other similar guidance, the VAF must be able to be updated with additional relevant information in the future.
- The VAF must be an integral part of long term physical and cyber investment strategies. Remediation costs become more manageable if part of an informed and comprehensive investment strategy.
- The VAF process must be repeatable over time. Today's VAF outcomes must be valid in tomorrow's investment climate.
- Senior Executive support in each Agency is crucial to making the VAF process a success.
- The VAF is not synonymous with penetration testing. Penetration testing may be a sub-element of the overall VAF procedures but should not be considered the recommended method for identifying vulnerabilities.

Scalability of the Framework

The VAF process is designed to be scalable, and the concepts applicable, to the identification of vulnerabilities at the National level, the Agency and Department level, and the internal process level of the organization. The questionnaires utilized in the VAF are best applied once the VAF team has clearly defined the processes in the organization that are considered the Mission Essential Processes. The scalability applies to a process whether the process is between the government and industry partners or internal to an agency.



II. The VAF Approach

In order to identify the critical infrastructure vulnerabilities that exist in, or impact upon, your organization, the assessment team should follow the assessment methodology detailed below. The methodology primarily consists of three major steps, as shown in Figure 1. Each step consists of a series of activities, which are outlined in the following sections. Using these assessment steps, the assessment team will compile a list of vulnerabilities for the organization to evaluate and determine appropriate next steps. Next steps include determining the order in which vulnerabilities should be addressed, the resources required, and the level of investment necessary to meet the President's objectives.

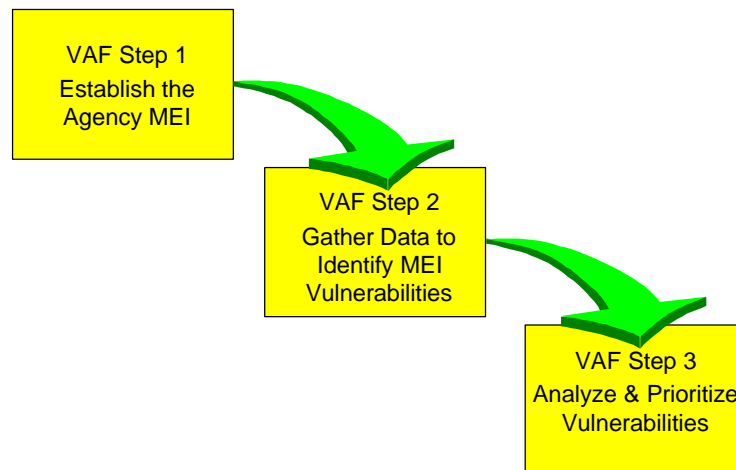


Figure 1. The VAF Steps

In Step 1 the assessment team will define the Minimum Essential Infrastructure for the organization. The focus is on the specific infrastructure components that support Mission Essential Processes (MEP) that are absolutely fundamental to achieving an organization's core mission. Once the MEI is identified, the vulnerabilities that potentially affect it are the most important starting points for infrastructure vulnerability minimization plans.

During Step 2 the VAF evaluation will review actions, devices, procedures, techniques and other measures that potentially place the organization's MEI resources at risk. The outcome will be the identification and reporting of flaws or omissions in controls (e.g. vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or the availability of resources that are essential to achieving the organization's core mission(s).

Finally in Step 3, the team will define and analyze the vulnerabilities identified in VAF Step 2 and MEI external dependencies from VAF Step 1, thereby enabling at least a first order of prioritization for purposes of remediation or minimization. This step will move the process from



CIAO

the vulnerability assessment phase into the first steps of the remediation planning process, with its accompanying funding estimates and timelines.

At a minimum, it is recommended that the first vulnerability assessment process consist of the broad, department- or agency-level macro vulnerability assessment of both the internal agency Minimum Essential Infrastructure (MEI), and the agency's relationship to, and connection with, the National MEI. Once the scope and MEI(s) are defined, the assessment team then can target VAF Steps 2 and 3 and focus on the appropriate core processes that are considered components of the critical infrastructure.

This detailed guide will serve as a scalable template for vulnerability assessment. The assessment team will determine the level of detail to which it should be applied and the analysis required to assess the MEI and its vulnerabilities.

Each step of the VAF will be outlined in the following format:

- Objectives
- Critical Success Factors
- Expected Outcomes
- Activities

Throughout this methodology, the assessment team will gather information through a number of data gathering activities including:

- Facilitated sessions
- On-site surveys
- Interviews
- Document reviews
- Validation activities to include procedural checks, system and process tests and simulations

The VAF assessment team has a responsibility to apply sound judgement in the data gathering process and to determine the usefulness and applicability of the questions and the control measures being reviewed. The questionnaires are derived from existing federal guidance and requirements already being used in the government. Most of the questions reflect a requirement or an audit control measure already being reviewed by the Agency or Department. The questionnaires are to be reviewed for applicability to the particular organization being assessed. If the team deems the measure or question does not apply, the rationale should be documented briefly and the question or control measure passed over.



III. VAF Step 1 - Establish the Minimum Essential Infrastructure (MEI)

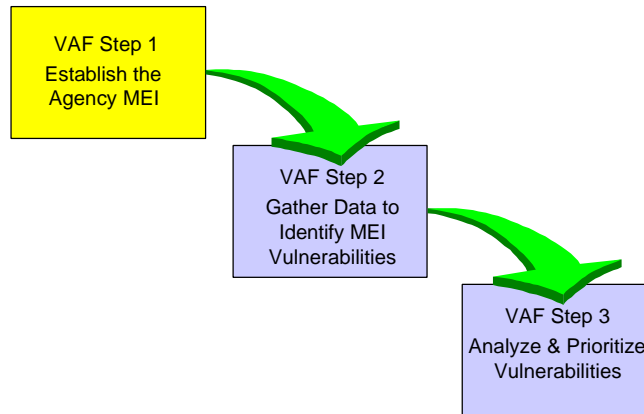


Figure 2. VAF Step 1

A. Objective

The objective of this step is to define the MEI for an organization. Let's first examine what MEI is, then what it is not, and finally, why the identification of MEI is the best starting point for this first-ever national vulnerability assessment process.

First, what does MEI mean? There are two levels that must be considered and assessed for this national VAF process to have value – the National MEI and the Agency MEI.



CIAO

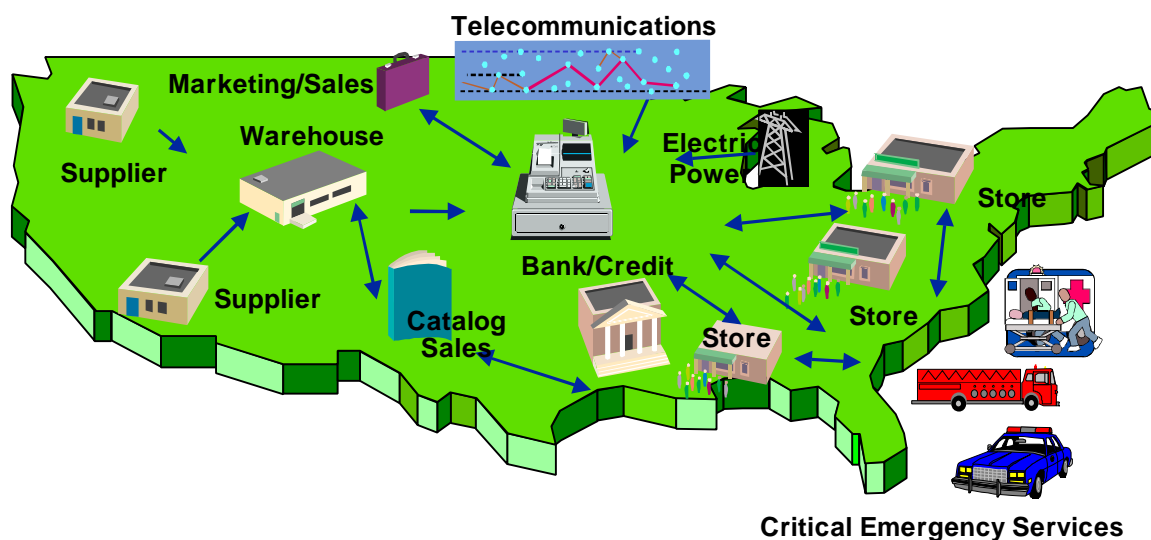


Figure 3. The National MEI

The *National MEI* is defined as the framework of critical organizations, personnel, systems, and facilities that provide a flow of goods and services that are absolutely essential to the economic well-being and national security of the United States, to the smooth functioning of governments at all levels, and to society as a whole.

The Agency MEI is the framework of critical organizations, personnel, systems, and facilities that are ***absolutely*** required in order to provide the inputs and outputs necessary to support the core processes, essential to accomplishing an organization's core mission as they relate to national security, national economic security or continuity of government services. In other words, the Agency MEI focuses on the specific infrastructure components that support Mission Essential Processes (MEP) as depicted in Figure 4 below that are absolutely fundamental to achieving an organization's core mission.

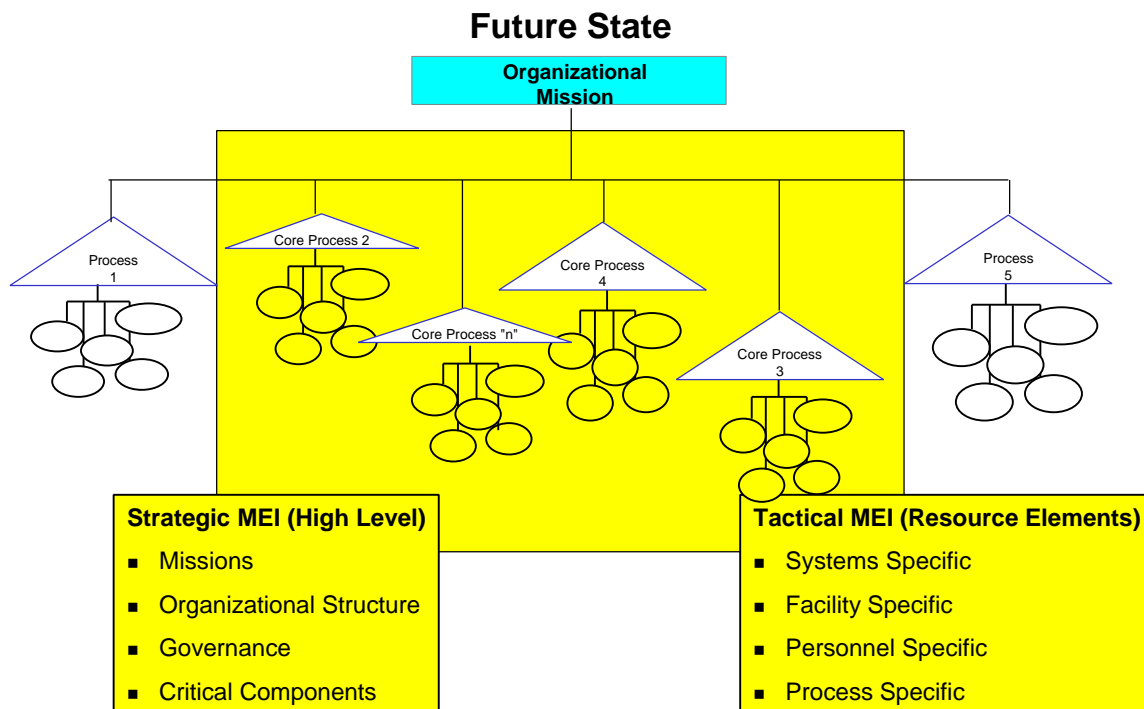


Figure 4. Defining MEI based on Core Processes of the Organization

Next, let's look at what the definition of MEI is not meant to include. In most cases the MEI is intended to be the absolute core component of what government agencies sometimes refer to as mission critical elements (MCE). Most agencies have defined their mission critical elements (MCE). The MCE are the resources needed to address each and every mission of the department or agency, regardless of their relevance to the core national security, national economic security requirements or continuity of government services of the United States.

The assessment team must determine the scope of the assessment in order to decide whether a National MEI, an Agency MEI or both need to be defined. Once the scope and MEI(s) are defined, the MEI(s) will allow the assessment team to target VAF Steps 2 and 3 and focus on the appropriate core processes that are considered components of the critical infrastructure.

Finally, why does the VAF process commence with an identification of the MEI? The answer is because it is the logical starting point. This will be discussed in greater detail below. In summary, by its very definition, the MEI represents the most essential elements supporting department or agency missions. So, once the MEI is identified, the vulnerabilities that potentially affect it are the most important starting points for infrastructure vulnerability minimization plans.



CIAO

B. Scope

In KPMG's initial meeting with the Critical Infrastructure Assurance Office staff following the award of the contract, it was emphasized that the VAF process must be scalable so that even inexperienced agencies would be able to use VAF, even if only at a very broad macro level. This VAF process lends itself to either such a macro level approach, or a detailed examination of every infrastructure issue within a department or agency.

At a minimum, it is recommended that this first vulnerability assessment process consist of the broad, department/agency level macro vulnerability assessment of both the internal agency MEI, and the agency's relationship to, and connection with, the National MEI. Once the scope and MEI(s) are defined, the MEI(s) will allow the assessment team to target VAF Steps 2 and 3 and focus on the appropriate core processes that are considered components of the critical infrastructure.

C. Process

In order to establish either type of MEI, the assessment team must first determine the *strategic MEI* which consists of a high level review of the:

- Mission(s),
- Organizational Structure,
- Governance, and
- High Level Definition of the Critical Components/Systems/Facilities/Processes.

Once the strategic level MEI is established, the *MEI* resource elements (or as some may say, the tactical MEI) can be examined. Essential resource elements include the following:

People	Staff, management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission. Security management personnel should also be included.
Technology	All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.
Applications	All application systems, internal and external, utilized in support of the core process.



CIAO

Data All data (electronic and hard copy) and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital/communication's channel.

Facilities All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above.

Subsets of resource elements are those elements critical to supporting the MEI. These are MEI resource elements.

D. Critical Success Factors

In order for this step to be successful, the following elements need to exist:

- ✓ Organizational commitment to the principles of PDD 63
- ✓ Application and assignment of the appropriate and knowledgeable personnel to the process of defining the MEI
- ✓ A solid understanding of the definitions of MEI
- ✓ A trained assessment team capable of assembling the information

E. Outcomes

The result of VAF Step 1 will be a comprehensive definition of the MEI for which the vulnerability assessment process will be applied.



F. Team Composition

In order to carry out the execution of this framework, the organization should establish a group of at least ten experts that could be broken into two teams based on the requirements and size of the effort. The minimal team should be comprised of the following experts:

Expertise	Description	Number Required
Project/Team Leader	Skilled in IT Auditing methodologies	2
Personnel Security, Training and Education	Past experience with personnel security issues such as background investigations, training and awareness issues	1
Mainframes	Skilled in CA-Examine auditing tool with either RACF or ACF2 security front-end for MVS.	1
Database Management Systems	Skilled in DBMS administration in products such as Oracle, Sybase, DB2, Informix, etc.	1
Telecommunications/Unix	Should be trained Unix administrator and knowledgeable of TCP/IP, X.400 protocols	2
Information Security	Should be knowledgeable in Orange Book requirements, life cycle management, continuity of operations, and security administration with some experience in using tools such as KAS, ISS, COPS, etc.	1
Networks	Skilled in LAN applications (i.e. Novell, NT, Banyan, etc) preferably trained in Systems Administration	2



CIAO

G. Activities Overview

There are primarily nine activities necessary to complete this step.

- 1.1 Identify the core mission(s) of the organization
- 1.2 Identify the threat environment
- 1.3 Identify the core processes supporting the core mission(s)
- 1.4 Analyze the value of each core process, categorizing them as *Code Red*, *Code Amber*, and *Code Green*
- 1.5 Identify organizational structure and customers as well as roles and responsibilities
- 1.6 Identify facilities
- 1.7 Map architecture and systems
- 1.8 Link physical, organizational and architecture components to core processes valued “*Code Red*”
- 1.9 Identify external resources upon which the department/agency MEI is dependent



CIAO

VAF Step 1.1 – Identify the core mission(s) of the organization

Description:

In order to assess the vulnerabilities of and protect its critical infrastructure, the organization must understand and clearly define its mission(s).

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
✓	Facilitated Sessions	Executive Leadership
✓	Interviews	Executive Leadership
✓	Document reviews	Strategic Plan
	Validation activities to include procedural checks, system and process tests and simulations	

Outcomes:

The core mission(s) of the organization is/are clearly defined and agreed upon by executive management.



VAF Step 1.2 – Identify the threat environment

Description:

The identification of the agency's high level threat in order to focus management on security environment in which it must operate. At a minimum, a definition of threat should include any circumstance or event with the potential to cause harm to an essential resource element through, at least, the following criteria:

- Denial of access to essential resource elements, i.e., denial of service
- Disruption of any service provided by essential resource elements to the extent that its availability is no longer assured
- Destruction of essential resource elements
- Deception – creating lack of confidence in essential resource elements
- Espionage or other harmful disclosure through or about resource elements , to include sensitive information or essential resource elements passed to, used or accessed by unauthorized persons/processes or in an unauthorized manner

The focus here is to develop or heighten the level of awareness by senior management of the potential threats to which the agency may be exposed. The evaluation of threats should include the general as well as the unique threats to which a particular agency is exposed.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
✓	Facilitated Sessions	Executive Leadership Security Management
✓	Interviews	Executive Leadership Security Management
✓	Document reviews	Existing Threat Assessments Existing Vulnerability Risk Assessments
	Validation activities to include procedural checks, system and process tests and simulations	



CIAO

Outcomes:

Awareness by senior management of the threats that exist to their strategic mission(s) and the motivations which may cause individuals, groups, or nations to take actions that may threaten this mission(s). This awareness will contribute to the analysis of the vulnerabilities identified in VAF Step 2. Also, this awareness will play a role in the development of the agency's strategic plan and the assessment of the agency's strategic and tactical MEI.

As with the PCCIP, PDD 63 is intended to address vulnerabilities to intentional acts. When considering the threat environment for such intentional acts, consideration should be given to potential threat sources and potential threat motivations. At a minimum, this step should include consideration of at least the following areas, plus any others more directly linked to department/agency missions and responsibilities.

Potential Threat Sources

- Nations (hostile or otherwise)
- Intelligence Services/Economic Competitors
- Sub or Transnational Groups
 - Terrorism/Damage
 - Organized Crime
- Non Traditional Threats
 - Weapons of Mass Destruction
 - Information Warfare
- Malicious *Code*, intentionally transferred or otherwise
- Threats to Personal Privacy
- Environmental Factors (debris, smoke, water, heat, electrical)
- Unwitting Third Parties
- Disgruntled Insiders
 - Employees
 - Contractors
 - Service Personnel
- Hackers and Vandals
- Common Crime, i.e., Fraud, Theft, etc.



Potential Threat Motivations

- Economic Gain
- Revenge
- Political Objectives
- Extortion
- Competitive Advantage
- Invasion of Privacy
- Meet a Challenge

The following may provide some structure in estimating both the probability and the impact of the potential threats a department or agency may consider in VAF Step 1.2.

Type of Threat	Probability	Impact
	Very Low – Very High	Low-Medium-High
	Very Low – Very High	Low-Medium-High
	Very Low – Very High	Low-Medium-High
	Very Low – Very High	Low-Medium-High

This analysis is a very high level analysis. The main intent of this activity is to increase awareness of the organization concerning the threat environment. The product of this threat analysis will be used in VAF Step 3.4 to review and analyze identified vulnerabilities in relation to the threat environment.



CIAO

VAF Step 1.3 – Identify the processes supporting the strategic or core mission(s)

Description:

The core processes that support the core mission(s) must be identified whether strategic, operational, administrative or otherwise. The appropriate team of knowledgeable individuals must be involved in this task.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
✓	Facilitated Sessions	Executive Leadership Security Management Functional Management Technical Management
✓	Interviews	Executive Leadership Security Management Functional Management Technical Management
✓	Document reviews	Tactical Plans Continuity of Operations Plan Response Plans Modernization Plans Personnel Policies and Plans
	Validation activities to include procedural checks, system and process tests and simulations	

The facilitated sessions should validate the critical components of each core process considered.

Outcomes:

Supporting processes are defined and linked to mission(s) they support.



CIAO

VAF Step 1.4 – Analyze the value of each core process

Description:

This activity refines the list of core processes down to those processes, which if not available, would cripple the organization to the point it could not achieve its mission.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
✓	Facilitated Sessions	Executive Leadership Security Management Functional Management Technical Management
✓	Interviews	Executive Leadership Security Management Functional Management Technical Management
	Document reviews	
	Validation activities to include procedural checks, system and process tests and simulations	

1. Analyze each core process and identify its value to the organization

After the core processes have been identified in VAF Step 1.3, a designated group of knowledgeable, management-level individuals should further analyze each core process. The analysis should consider whether each individual process, if lost, would:

- *Code Red*: Prevent the Agency from fulfilling its mission, critical national security or national economic security functions or from providing continuity of core government services. From the perspective of an attacker, this would constitute a “Kill.”
- *Code Amber*: Significantly debilitate or interfere with the ability of the Agency to fulfill its mission, critical national security or national economic security functions or provide continuity of core government services.
- *Code Green*: No appreciable impact on agency missions.



CIAO

2. After categorizing the core processes utilizing the above criteria, review the categorization to perfect the value assignment. Then, examining all the processes categorized as *Code Amber* or *Code Green*, assess whether in aggregate within the respective category, a series of these disabled processes would prevent the Agency from fulfilling its mission or supporting the national MEI, thus making them in the aggregate a *Code Red*.
3. The organization must also consider the time variable. The agency must review the processes categorized or valued at the *Amber* or *Green* level against a variable of time. If the process escalates to next higher value over time, the agency should consider whether the process should be included in the MEI. For example, a process may be valued at *Amber* if in the first few hours of loss it will significantly debilitate or interfere with the ability of the Agency to fulfill its mission. If over the next few hours or days, loss of the process will prevent the Agency from fulfilling its mission, critical national security or national economic security functions or from providing continuity of core government services, the value of the process should be considered *Code Red*.

Outcomes:

A list of core processes that have the highest priority in order to fulfill the mission of the organization or support the National MEI.



CIAO

VAF Step 1.5 – Identify organizational structure and customers

Description:

The human element is always a critical consideration. This is not only because of the value our society places on human life, but because certain personnel are in key positions with key skills who may not have appropriate backup and may not be easy to replace. This activity strives to identify those people who are involved in each core process and the role they play. The focus here is to highlight the key roles in the organization.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
	Facilitated Sessions	
✓	Interviews	Security Management Functional Management Technical Management
✓	Document reviews	Disaster Recovery Plan Personnel Security Plans Clearance Process Key Personnel Listing Organizational Structure Continuity of Operations Access Rosters
	Validation activities to include procedural checks, system and process tests and simulations	

Having evaluated each core process in VAF Step 1.4, this VAF Step provides a framework for assessing the role of specific personnel in supporting those core processes. One essential analytical function is to determine whether there is sufficient trained staff to perform core processes in the threat environment of the department or agency. Just as there can be single points of failure for equipment and facilities, there can be human resource single points of failure. This analytical step should address that issue.

Outcomes:

Key players in core processes and security management are defined.



CIAO

VAF Step 1.6 – Identify facilities

Description:

This activity identifies the facilities upon which the organization depends and the role those facilities play in supporting core processes. These facilities may be owned and operated by the organization or may be outsourced and maintained by a third party.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
	Facilitated Sessions	
✓	Interviews	Facility Management Security Management
✓	Document reviews	Disaster Recovery Plans COOP Physical Layouts Modernization Plans Response Plans
	Validation activities to include procedural checks, system and process tests and simulations	

The purpose of this analysis is to assess the impact of loss on core mission functions of each facility individually, or two or more linked facilities.

Outcomes:

Facilities are identified and their roles in support of the core processes are defined.



VAF Step 1.7 – Map cyber architecture, data and systems

Description:

Identifying and defining the components in the organization's system, data, and information architecture aids in the full depiction of the organization's resources.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
	Facilitated Sessions	
✓	Interviews	Technical Management Security Management
✓	Document reviews	Information Architecture Network Architecture Information Security Plans Training Plans System Inventory Data Inventory
	Validation activities to include procedural checks, system and process tests and simulations	

The architecture and mapping should include documentation of:

- **Major applications** – Systems that perform clearly defined functions. A major application might comprise hardware, software and telecommunications components. These components can be a single software application or a combination of hardware/software focused on supporting a specific mission related function. A major application may also consist of multiple individual applications, related to a single mission function (e.g. payroll or personnel). If a system is defined as a major application and the application is run on another organization's general support system" than the interdependencies should be defined.



CIAO

- **General Support Systems** – Interconnected systems that share common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people; and provides support for a variety of users and applications. A general support system, for example, can be a:
 - LAN
 - Backbone
 - Communications network
 - Departmental data processing center including its operations center and utilities
 - Tactical radio network
 - Sharing information processing service organization
- **Sensitivity of the Information Handled** – documentation of the sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system. The sensitivity of the information handled should be evaluated based on:
 - Confidentiality – the system contains information that requires protection from unauthorized disclosure.
 - Integrity – the system contains information, which must be protected from unauthorized, unanticipated or unintentional modification.
 - Availability – the system contains information or provides services which must be available on a timely basis to meet mission requirements or to avoid substantial losses.
- **Interfaces and Information Sharing** – a detailing of the types of interfaces between systems and the types of information flowing between the internal applications and with external systems. Documentation of the authorizations for this type of information sharing should also be included.

Outcomes:

The organization's architecture and its components are defined.



CIAO

VAF Step 1.8 – Link physical, organizational, architecture components to the core processes that play key roles in achieving the mission

Description:

This activity pulls together the information gathered in activities 1.5, 1.6, and 1.7 and sorts it by the definitions and criteria for *Codes Red*, *Amber*, and *Green* in activity 1.4. The intent is to narrow the scope to the minimum essential resource elements necessary to support the core processes from the larger scope of all the resource elements that support the whole organization and all of its processes.

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
	Facilitated Sessions	
✓	Interviews	Executive Leadership Security Management Technical Management Functional Management
✓	Document reviews	Documents from VAF Step 1 – Activities 1.5, 1.6, and 1.7
	Validation activities to include procedural checks, system and process tests and simulations	

The analytical process in Step 1.8 comes after the results of Steps 1.4, 1.5, 1.6, and 1.7 are compared. The purpose of the analysis is to identify those physical, cyber and human resources that are so crucial to the ability of the department or agency to perform its core mission that the mission cannot be performed without them. This analysis should result in the identification of a department or agency's MEI.

Outcomes:

An accurate representation of the minimum essential resource elements that support each of the core processes essential to performing the core mission(s) of the department or agency.



VAF Step 1.9 – Identify the external resources upon which the MEI is dependent.

Description:

Presidential Decision Directive (PDD) 63 instructed that the government and sectoral vulnerability assessment plans include a particular focus on interdependencies. So, it is important to understand what the term “interdependency” means and how it should apply to the vulnerability assessment plans of government departments and agencies.

The term “interdependencies” was used by the PCCIP primarily as a verbal shorthand for the way in which interconnected networks have made infrastructure components dependent upon one another in ways not heretofore experienced.

Historically, the nation’s critical infrastructures have primarily been physically separate systems. Today, these infrastructures are increasingly dependent upon the automated control networks that link them together, sometimes controlling how they interact with each other. Thus, the failure of a component in one infrastructure may cause a cascade of failure into one or more other infrastructures. As a result, these linkages between and among infrastructures have created a new dimension of vulnerability, e.g., interdependence. These interdependencies, combined with the new environment of unconventional threats, pose a new, mostly unrecognized, area of national and business risk.

There a number of new forces in the marketplace that the PCCIP believed potentially increase the potential negative impact of infrastructure interdependencies. One is system complexity, and a second is deregulation.

The complexities of interconnected infrastructure control systems add to the challenge of recognizing interdependencies. Complex system control software, network architecture and/or other related factors can mask flaws that will contribute to cascading failures across multiple infrastructures. For example, in the energy infrastructure, this could mean that a rather minor or routine disturbance would cascade into a regional outage. Without electric power, other critical infrastructures, such as telecommunications and banking and finance begin to feel the impact, particularly if the period of outage continues beyond a short period. In fact, nearly every infrastructure may begin to feel the impact of what began as a relatively minor problem.

In addition to complexities, deregulation can introduce new interdependencies to an industry’s traditional risk management models. In telecommunications and, increasingly, electrical power, multiple intermediaries have been inserted into what once were end-to-end service systems that—when combined with decreases in reserve capacity margins in these industries resulting from competitive cost pressures—make the operational interdependency among these two gigantic infrastructures even more opaque and complicated.



CIAO

Necessary Data Gathering:

	Data Gathering Activity	Targeted Participants and Products
✓	Facilitated Sessions	Executive Leadership Security Management Technical Management Functional Management
	Interviews	
	Document reviews	
	Validation activities to include procedural checks, system and process tests and simulations	

Once the MEI resource elements have been clearly defined through the preceding activities, this activity will force the organization to identify where the MEI is dependent on resources and services outside the organization's control. For the purposes of VAF Step 1, the issue of interdependencies is addressed at the high-end macro level. However, particular attention should be paid to the MEI resource elements that may be outsourced, and, thus, may be partially under the control of the Agency through contractual means. When MEI resource elements are identified that are completely outside the control of the Agency, they should be carefully evaluated in VAF Step 3 in light of the other vulnerabilities that come out of VAF Step 2.

MEI Dependencies			
	Internal Resources	External Resources (control)	External Resources (no control)
People			
Technology			
Applications			
Data			
Facilities			

Outcomes:

Internal and External Interdependencies are identified for consideration in VAF Step 2 and analysis in VAF Step 3.



IV. VAF Step 2 - Gather Data to Identify MEI Vulnerabilities

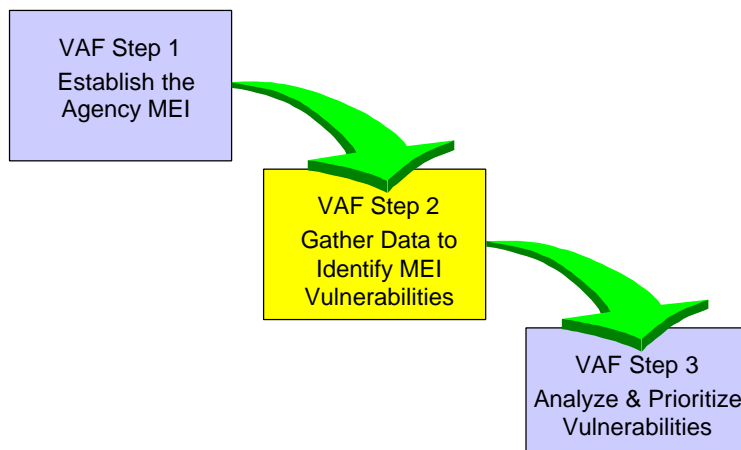


Figure 5. VAF Step 2

A. Objective

The objective of this step is to identify the vulnerabilities in the organization related specifically to the MEI identified through VAF Step 1.

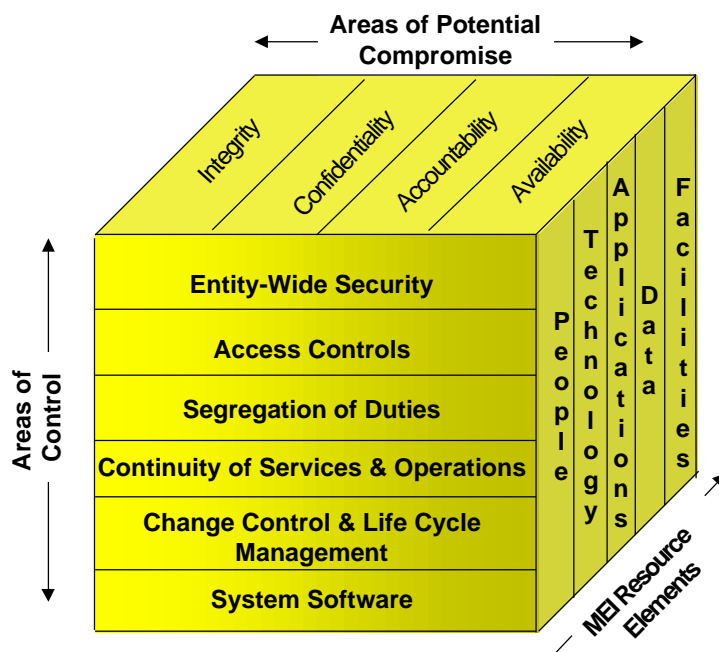


Figure 6. The VAF Cube



CIAO

As noted previously, some suggest that penetration testing is an adequate approach to the cyber portion of VAF. As will be seen from this VAF process, a much broader approach is necessary to produce a comprehensive cyber vulnerability identification mechanism. Penetration testing has its place in that process, but falls well short of being a “silver bullet” for infrastructure vulnerability assessments. A review of root causes of infrastructure vulnerability is necessary before any meaningful effort to minimize those vulnerabilities can be undertaken.

The criteria used to identify these vulnerabilities are depicted in Figure 6 – The VAF Cube. The cube consists of three faces, defined as follows:

Areas of Control:

Collectively, controls consist of the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. The control areas set out in the KPMG VAF process have been modified from GAO’s FISCAM standards for auditing federal information systems. The FISCAM definitions of the control areas have been expanded for this VAF process to incorporate infrastructure vulnerability issues.

MEI Resource Elements:

As previously discussed, these are the broad categories of resources, all or portions of which, constitute the minimal essential infrastructure necessary for a department, agency or organization to conduct its core mission(s). These resource elements are very similar to, but modified somewhat from, the COBIT™ framework used by ISACF. The definitions have been expanded to incorporate physical infrastructure vulnerability areas.

Areas of Potential Compromise:

These broad topical areas represent categories where losses can occur that will impact both a department or agency’s MEI and its ability to conduct core missions.

The KPMG VAF process examines the adequacy of department or agency Areas of Control set out on the VAF cube Face 1. The process is designed to measure an organization’s effectiveness in protecting the MEI Resource Elements listed on VAF cube Face 2. This mechanism will result in the identification of Areas of Potential Compromise listed on VAF cube Face 3. The result will be categorized vulnerability listings, directly related to the MEI and for which minimization strategies may be necessary, probably to include modifications to organizational control mechanisms.



CIAO

Stated another way, the VAF evaluation will review actions, devices, procedures, techniques and other measures that potentially place the organization's MEI resources at risk. The outcome will be the identification and reporting of flaws or omissions in controls (e.g. vulnerabilities) that may affect the integrity, confidentiality, accountability, and/or the availability of resources that are essential to achieving the organization's core mission(s).

The three-way cross cut of issues represented by the VAF cube, which incorporates both physical and cyber issues, represents a unique approach to the process of identifying vulnerabilities created by systemic flaws in control and management of critical resources. The identification of such systemic flaws allows remedies to be applied at a systemic level, thereby maximizing the impact of remediation efforts.

Face One – Areas of Control

- Entity-Wide Security - Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.
- Access Controls - Procedures and controls that limit or detect access to MEI Resource Elements (People, Technology, Applications, Data and/or Facilities) thereby protecting these resources against loss of Integrity, Confidentiality Accountability and/or Availability.
- Segregation of Duties - Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to MEI Resource Elements.
- Continuity of Service and Operations - Controls to ensure that, when unexpected events occur, departmental/agency MEI services and operations, including computer operations, continue without interruption or are promptly resumed and critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.
- Change Control & Life Cycle Management - Procedures and controls that prevent unauthorized programs or modifications to an existing program from being implemented.
- System Software - Controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system.



CIAO

Face Two – MEI Resource Elements

These Resource Elements have been defined earlier in the process, but will be repeated here for continuity purposes. They are:

- People - Staff, management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission. Security management personnel should also be included.
- Technology - All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.
- Applications - All application systems, internal and external, utilized in support of the core process.
- Data - All data (electronic and hard copy) and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital/communication's channel.
- Facilities - All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above.

Face Three – Areas of Potential Compromise

In reviewing the areas of control against the MEI resource elements, if vulnerabilities are identified, it would mean controls are not in place to ensure the following:

- Integrity - The accuracy, completeness and reliable transmission and reception of information and its validity in accordance with business values and expectations; the adequacy and reliability of processes assuring personnel selection, access and safety; and the adequacy and reliability of processes assuring authorized access to and the safety of physical facilities.
- Confidentiality - The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.



CIAO

- Availability - The ability to have access to MEI Resource Elements when required by the mission and core supporting process(s), both now and in the future. It also concerns the safeguarding of those resources and associated capabilities.
- Accountability - The explicit assignment of responsibilities for ownership and/or oversight of the process, system, as well as inputs and outputs. Accountability may be assigned at various levels within the organization to include executives, managers, staff, system, information or facilities owners, providers, and users of MEI Resource Elements. These assignments are reviewed for effectiveness and appropriateness in the areas of control listed on VAF Cube Face 1. In the management of vulnerabilities, accountability is imperative and as an area of compromise is highlighted in VAF Step 3.



CIAO

VAF Step 2 – Inputs

- Policy
- Procedures
- Plans
- Organization of Agency
- Architecture Components (Physical and Cyber)

VAF Step 2 – Input Examples

The following items are representative of the types of documentation needed to conduct the assessment:

- Physical Security Plans
 - Facility
 - Vulnerability Risk Assessment
 - Threat Analysis
 - Procedures and Policies
 - Modernization Plans
 - Response Plans and Capabilities
 - Continuity of Operations Plans
- Personnel Security Plans
 - Clearance Process
 - Key Personnel Identification
 - Organizational Structure
 - Continuity of Operations Cross Training and Practice
 - Access Controls Rosters
 - Key Element Analysis
- Training Plans
 - Inventory of Classes
 - Physical and Cyber Security Awareness Training
 - Certification and Accreditation Program
 - Emergency Response and Crisis Management Training



CIAO

- Security
 - Security Concept of Operations (CONOPS) and Practice (specific to applications and facilities)
 - Security Mode Determination
 - Security Test and Evaluation
 - Emergency Response Capabilities and Practice
- Cyber Plans
 - Architecture and Access
 - Security and Oversight
 - Training and Awareness
 - Systems Inventory and Access Control
 - Data Inventory and Access Control
 - Continuity of Operations and Reconstitution
 - Proactive system integrity monitoring and emergency response capabilities

B. Critical Success Factors

In order to successfully use the cube, the assessment team must:

- ✓ Have full support from executive management
- ✓ Use a clearly defined MEI
- ✓ Have access to the appropriate staff and existing documentation (plans, policies and procedures)

C. Outcomes

A list of vulnerabilities:

- Classified by Core process and by Area of potential compromise
- Illustrating interdependencies and potential impact

D. Scalability of the Process

The VAF process was designed to be scalable, and the concepts applicable, to the identification of vulnerabilities at the National Level, the Agency/Department Level and internal process level of the organization. The questionnaires utilized in VAF Step 2 are best applied once the VAF team has clearly defined the process to be examined and the associated MEI Resource Elements. The scalability applies to the process whether the process is maintaining EC between the government and industry trading partners or maintaining communications within an agency.



The questionnaires in VAF Step 2 are derived from existing federal guidance and requirements already being utilized in the government. Most of the questions reflect a requirement or an audit control measure being reviewed by the Agency/Department auditors. The questionnaires are to be reviewed for applicability to the particular organization being assessed. The VAF team has a responsibility to apply sound judgement in the data gathering process and determining the usefulness and applicability of the questions and the control measures being reviewed. If the team deems the measure or question does not apply, the rationale should be documented briefly and the question or control measure passed over.

E. Activities

The activities that comprise this step are essentially the data gathering and analyses necessary to evaluate each of the six areas of control. Each area of control has an assessment questionnaire designed to gather information pertinent to that area of control. The assessment team would perform the data gathering and analysis required in the six areas of control detailed in the following pages.

Each control area questionnaire is structured based on the following outline:

<i>Topical Areas:</i>	A grouping of related control objectives.
<i>Control Objectives:</i>	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.
<i>Questions On Controls:</i>	The policies and procedures and practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.

The questionnaires for each control area are provided in Appendices A-F of this guideline document.

The VAF team based on VAF Step 1 will have documented each process and the associated MEI Resource Elements. Based on the process list, the VAF team should examine each process utilizing the VAF cube approach. The six questionnaires that are used in this step are scalable. The VAF team should approach using each questionnaire based on the MEI level and organization being examined.



CIAO

The team should apply best judgement in the detail required from the questionnaires provided. The questionnaires are comprehensive and assume a team who is well versed in the required level and format of documentation as well as the terminology being applied.

The team should apply greater scrutiny using certain sections of the questionnaire based on the type of process being reviewed. For example, if the team is examining a process utilizing or consisting of a predominant cyber component, the sections of the questionnaire, which addresses physical/facility, control measures should be minimized.

If the organization is already performing vulnerability assessments, the team should examine the process being used against the VAF process and determine if gaps between the two exist. The intent of the VAF process is to use, if available, existing data gathering and analysis techniques in the identification and documentation of vulnerabilities in the infrastructure. The intent is not to duplicate existing efforts.

The results of the questionnaires should be gathered in a secure database for future analysis.



VAF Step 2.1 – Assess Areas of Control – Entity Wide Security

Description:

Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls and physical security controls.

An entity-wide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program should establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well-designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources, e.g. vulnerabilities and disproportionately high expenditures for controls over low-risk resources.

Interviews and Data Gathering:

See Questionnaire in Appendix A.

To gather the information required in the questionnaire, the VAF team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated process and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the VAF team should meet with the staff responsible for setting policy and procedures and to identify those policies and procedures that are defined. The VAF team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify they are being followed.



CIAO

Areas of Concern:

It is essential that the security program planning and management organization provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's computer-related controls.

The critical elements in developing and implementing an entity-wide security program involve factors that are essential to several internal control components, including the control environment. Therefore, these critical elements help ensure the effectiveness of the entity's overall internal control. The relevant factors include supportive attitudes and actions by senior management, ongoing assessments of risk and monitoring of related policies, and effective communications between management and staff. All internal control components should be present and functioning effectively to conclude that internal control is effective. However, the control environment sets the tone of the organization. Generally, a specific control technique, including penetration testing, or group of techniques cannot be relied on to be effective on an ongoing basis unless it is supported by a strong control environment. For this reason, the auditor should be cognizant of control environment factors throughout the audit and adjust audit procedures accordingly.

Control Objectives:

Risk Management

Risk assessments should consider data sensitivity and the need for integrity and the range of risks that an entity's MEI resource elements may be subject to, including those risks posed by authorized internal and external users, as well as unauthorized outsiders who may try to "break into" the cyber systems. Such analyses should also draw on reviews of system and network configurations and observations and testing of existing security controls for cyber systems, as well as reviews and testing of controls for the other resource elements.

Entity-Wide Security Program Plan

Entities should have a written plan that clearly describes the entity's security program and policies and procedures that support it. At a minimum, the plan and related policies should cover all MEI resource elements and outline the duties of those who are responsible for overseeing security (the security management function) as well as those who own, use, or rely on the entity's computer and physical resources.

Security Management Structure

Senior management should establish a structure to implement the security program throughout the entity. The structure generally consists of a core of personnel who are designated as security



CIAO

managers. These personnel play a key role in developing, communicating, and monitoring compliance with security policies and reporting on these activities to senior management. The security management function also serves as a focal point for others who play a role in evaluating the appropriateness and effectiveness of computer-related controls on a day-to-day basis. These include program managers who rely on the entity's computer systems, system administrators, and system users.

However, because security is not an end in itself, senior managers should balance the emphasis on security with the larger objective of achieving the entity's mission. To do this effectively, top management should understand the entity's security risks and actively support and monitor the effectiveness of the entity's security policies. If senior management does not monitor the security program, it is unlikely that others in the organization will be committed to properly implementing it.

Effective Security-Related Personnel Policies

Policies related to personnel actions, such as hiring and termination, and employee expertise are important factors for information and facility security. If personnel policies are not adequate, an entity runs the risk of:

- (1) hiring unqualified or untrustworthy individuals,
- (2) providing terminated employees opportunities to sabotage or otherwise impair entity operations or assets,
- (3) failing to detect continuing unauthorized employee actions,
- (4) lowering employee morale, which may in turn diminish employee compliance with controls, and;
- (5) allowing staff expertise to decline.

Outsourcing

Vendor management controls involve the definition of procedures, the services to be provided, adherence to agreements and service levels, and qualifications of personnel.

Electronic Commerce

Electronic commerce controls involve the management of contractual, standards for transactional security, and authentication using certificate authorities.

Interdependencies

Important considerations in managing entity-wide security are the resultant risks to organizational entities as the result of interdependencies of forces both internal and external to the organization. Examples of internal and external interdependencies are labor strikes for outsourced service



CIAO

providers or contractual difficulties by service providers, in addition to externally provided utilities and other critical infrastructures.

Control Objective Topical Areas:

- Organizational Management
- Risk Assessment
- Security Plans
 - Security Policy
 - Current State of Security
 - Requests for Access
 - Accountability
 - Update on Plan
 - Organizational Goals
 - Commitment to Security
 - Limits of Security
- Security Management Structure & Responsibilities
- Security-Related Personnel Policies
 - Ensure Personnel Have Proper Security Clearances and/or Access Authorizations
 - Ensure Users Are Educated in Security Responsibilities
 - Maintain Records of Valid Security Clearances and/or Access Authorizations
 - Ensure Maintenance Personnel Have Proper Clearances and Access
- Security Program Effectiveness
 - Be Aware of Directives, Regulations, Policies and Guidelines
 - Participate in Developing Site Specific Documents
 - Provide Input to Other Security Documents (incident reports, inventories, vulnerability reports, response plans, COOP plans, etc.)
- Security Awareness
 - Ensure All Personnel Have Security Awareness Training
 - Ensure Users Are Trained in Proper Use of Passwords
 - Ensure Users Monitor Their Logins
 - Ensure Users Know How to Report Problems
 - Promulgate Awareness Information

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



VAF Step 2.2 – Assess Areas of Control – Access Controls

Description:

Procedures and controls that prevent unauthorized programs or modifications to an existing program from being implemented, or physical procedures and controls that prevent unauthorized access to or within physical facilities.

Access controls provide reasonable assurance that resources (data files, application programs, and computer-related facilities and equipment) are protected against unauthorized modification, disclosure, loss, or impairment. Such controls include physical controls, such as keeping computers in locked rooms to limit physical access, and technical controls, such as security software programs designed to prevent or detect unauthorized access to sensitive files.

Interviews and Data Gathering:

See Questionnaire in Appendix B.

To gather the information required in the questionnaire, the VAF project team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated processes and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF project team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the project team should meet with the staff responsible for setting policy and procedures and identify those policies and procedures that are defined. The project team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify that they are being followed.

Areas of Concern:

Access is based on one or more of three user characteristics:

- Something a person knows – password, Personal Identification Number (PIN)
- Something a person has – smart card, bank card, key, pass card
- Something a person is – based on personal characteristics (biometrics)



CIAO

The objectives of limiting access are to ensure that:

- users have only the access needed to perform their duties,
- access to very sensitive resources, such as security software programs or the main console in the data center, is limited to very few individuals, and
- employees are restricted from performing incompatible functions or functions beyond their responsibility.

If these objectives are met, the risk of inappropriate modification or disclosure of data can be reduced without interfering with the practical needs of users. However, establishing the appropriate balance between user needs and security requires a careful analysis of the criticality and sensitivity of information resources available and the tasks performed by users.

Discretionary control is the most common type of access control mechanism implemented in computer systems today. The basis of this kind of security is that an individual user, or program operating on the user's behalf, is allowed to specify explicitly the types of access other users (or programs executing on their behalf) may have to information under the user's control.

Discretionary security differs from mandatory security in that it implements the access control decisions of the user. Mandatory controls are driven by the results of a comparison between the user's trust level or clearance and the sensitivity designation of the information.

Discretionary controls are not a replacement for mandatory controls. In any environment in which information is protected, discretionary security provides for a finer granularity of control within the overall constraints of the mandatory policy. Both discretionary and mandatory controls can be used to implement an access control policy to handle multiple categories or types of information, such as proprietary, financial, personnel or classified information. Such information can be assigned different sensitivity designations and those designations enforced by the mandatory controls. Discretionary controls can give a user the discretion to specify the types of access other users may have to information under the user's control, consistent with the overriding mandatory policy restrictions. In a classified environment, no person may have access to classified information unless: (a) that person has been determined to be trustworthy, i.e., granted a personnel security clearance – MANDATORY, and (b) access is necessary for the performance of official duties, i.e., determined to have need-to-know – DISCRETIONARY. (For a further discussion of these concepts refer to the Department Of Defense Standard, Department Of Defense Trusted Computer System Evaluation Criteria, December 1985.)

Control Objectives: Security policies defined for systems, including those that are used to process classified or other sensitive information, should include provisions for the enforcement of discretionary access control rules. That is, they must include a consistent set of rules for controlling and limiting access to identified users who have been appropriately authorized to have access to particular resources.



Data Classification

Resource owners should determine the level of protection that is most appropriate for the resources for which they are responsible. These determinations should flow directly from the results of risk assessments that identify threats, vulnerabilities, and the potential negative effects that could result from disclosing confidential data or failing to protect the integrity of data supporting critical transactions or decisions. All resource classifications should be reviewed and approved by an appropriate senior official, maintained on file, and periodically reviewed to ensure that they reflect current conditions.

Implementing adequate access controls involves first determining what level and type of protection is appropriate for individual resources and who needs access to those resources. The resource owners should perform these tasks. For example, program managers should determine how valuable their program data resources are and what access is appropriate for personnel who must use an automated system to carry out, assess, and report on program operations. Similarly, managers in charge of system development and modification should determine the sensitivity of hardware and software resources under their control and the access needs of systems analysts and programmers. System administration officials should determine the access needs of system administration personnel.

Policies specifying classification categories and related criteria can help resource owners classify their resources according to their need for protective controls. The Computer Security Act requires agencies to identify systems that process “sensitive” data. “Sensitive” data is defined as “any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under [the Privacy Act.]” OMB Circular A-130, Appendix III, directs federal agencies to assume that all major systems contain some sensitive information that needs to be protected, but to focus extra security controls on a limited number of particularly high-risk or major applications.

Broad or special access privileges, such as those associated with operating system software that allow normal controls to be overridden, are only appropriate for a small number of users who perform system maintenance or handle emergency situations. Such special privileges may be granted on a permanent or temporary basis. However, any such access should also be approved by a senior security manager, written justifications should be kept on file, and the use of highly sensitive files or access privileges should be closely monitored by management.

Access Control Lists (ACL)

An entity should institute policies and procedures for authorizing access to information resources and documenting such authorizations. These policies and procedures should cover user access



CIAO

needed for routine operations, emergency access, and the sharing and disposition of data with individuals or groups outside the entity.

The computer resource owner should identify the specific user or class of users that are authorized to obtain direct access to each resource for which he or she is responsible. This process can be simplified by developing standard profiles, which describe access needs for groups of users with similar duties, such as accounts payable clerks.

The owner should also identify the nature and extent of access to each resource that is available to each user. This is referred to as the user's profile. In general, users may be assigned one or more of the following types of access to specific computer resources:

- Read access, which is the ability to look at and copy data or a software program.
- Update access, which is the ability to change data or a software program.
- Delete access, which is the ability to erase or remove data or programs.
- Merge access, which is the ability to combine data from two separate sources.
- Execute access, which is the ability to execute a software program.

Access may be permitted at the file, record, or field level. Files are composed of records, typically one for each item or transaction. Individual records are composed of fields that contain specific data elements relating to each record. Access authorizations should be documented on standard forms, maintained on file, approved by senior managers, and securely transferred to security managers. Owners should periodically review access authorization listings and determine whether they remain appropriate.

Listings of authorized users and their specific access needs and any modifications should be approved by the appropriate senior manager and directly communicated in writing by the resource owner to the security management function. A formal process for transmitting these authorizations, including the use of standardized access request forms, should be established to reduce the risk of mishandling, alterations, and misunderstandings. The security manager should review authorizations for new or modified access privileges and discuss any questionable authorizations with the authorizing official. Approved authorizations should be maintained on file.

It is equally important to notify the security function immediately when an employee is terminated or, for some other reason, is no longer authorized access to information resources. Who is responsible for notification? Policies should be in place clearly assigning responsibility for notifications whether it is the human resources department or another group. Terminated employees who continue to have access to critical or sensitive resources pose a major threat, especially those individuals who may have left under acrimonious circumstances.



Physical Controls

Physical controls are imposed by the organization upon the determination that specified resources require a certain level of protection. Overall, physical security should be reviewed based on the type of facility, i.e. geographic location, fragmented facilities, and public access facilities, as well as the location within the facility, i.e. lobbies, parking facilities, utility facility, and trash disposal facility. Special circumstances should also be considered, i.e. a facility is under construction or houses different types of personnel, in the case of a day care center.

Different facilities require different physical security controls related to interior, perimeters, entries, barriers and openings, protective lighting, intrusion detection systems (IDS) and key controls. Certain procedures and policy should be in place and appropriate techniques applied, i.e. security systems, electronic monitoring, and security screening.

The review of physical controls should also consider security, contract and custodial personnel, equipment, vehicles, communication techniques and training.

Data Centers

For a data center, controls should be in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.

Physical Access Lists and Visitor Logs to Data Centers

For a data center, controls should be in place to ensure that adequate control measures are imposed to safeguard equipment and facilities.

Physical keys, Card keys and Cipher locks

For all designated facilities, controls should be in place to ensure that adequate physical security measures are imposed to safeguard equipment and facilities.

Passwords

The use of passwords, tokens, or other devices are used to identify and authenticate users that have been designated a specific level of access. Procedures for maintenance and monitoring of passwords is imperative for secure access to be ensured.

Network Management Systems (NMS)

Security over local area networks (LAN) is required to adequately protect the resources that are utilized. In the same vein as a mainframe platform, a systems administrator must implement adequate controls to protect LAN resources from unauthorized use. This includes setting up user profiles and appropriately limiting dial-up or remote access to authorized personnel.



Security Software/Access Control Software

Security software can be used to ensure logical controls over data files and software programs. It can also be used to manage physical access over entry points to facilities, i.e. card keys.

Database Management Systems (DBMS)

DBMS have built in utilities and access features. The use of logical controls over a database in combination with capabilities provided through Network Management Systems (NMS) may provide power access control capabilities.

Remote Access

For systems that can be accessed through public telecommunications lines, some users may be granted dial-up access. This means that these individuals can use a modem to access and use the system from a remote location, such as their home or a field office. Because such access can significantly increase the risk of unauthorized access, it should be limited and the associated risks weighed against the benefits. To help manage the risk of dial-up access, justification for such access should be documented and approved by owners. Management must control resources and assets, under their responsibility, by implementing a formal process that tracks access granted and services/property distributed. It also applies to outsourced functions. Other telephony related topics include platforms relating to PBX, Voicemail and Call Detail Reporting systems.

Encryption and Related Applications

For certain types of data, the use of cryptographic tools may be imperative to ensure the protection of data during transport. In parallel, transaction authorization and cryptographic key management are applications that can be applied to certain communications and types of data.

Cryptography involves the use of algorithms (mathematical formulae) and combinations of keys (strings of bits) to do any or all of the following:

- Encrypt, or electronically scramble, a message or file so that it is unintelligible to those who do not have the secret key needed to decrypt it, thus keeping the contents of the message or file confidential.
- Provide an electronic signature that can be used to:
 - determine if any changes have been made to the related file, thus ensuring the file's integrity, and
 - link a message or document to a specific individual's or group's key, thus ensuring that the "signer" of the file can be identified.

Cryptographic tools are especially valuable for any application that involves "paperless" transactions or for which the users want to avoid relying on paper documents to substantiate data integrity and validity. Examples include:



CIAO

- electronic commerce, where purchase orders, receiving reports, and invoices are created, approved, and transmitted electronically,
- travel administration, where travel orders and travel vouchers are created, approved, and transmitted electronically, and
- protection of documents or digital images, such as contracts, personnel records, or diagrams, that are stored on electronic media.

Monitoring/Auditing

Monitoring measures need to be established to detect and ensure correction of security breaches, such that all actual and suspected breaches are promptly identified, investigated, and acted upon, and to ensure ongoing compliance with policy, standards, and minimum acceptable security practices. Monitoring should occur on a continuous basis to assess performance of implemented controls over time and ensure that identified deficiencies are reported to senior management in a timely manner.

Compliance with access authorizations should be monitored by periodically comparing authorizations to actual access activity. Access control software typically provides a means of reporting user access authorizations and access activity.

Monitoring activities may include maintenance of audit trails, continuous review of actual or attempted unauthorized, unusual, or sensitive access, investigation of and response to suspicious access activity as well as ongoing security surveillance activities.

Datascope and Sniffers

Network monitoring is a valuable tool in maintenance and review of access controls. Data entered at a workstation attached to a LAN is normally transmitted in clear text over the network. Any user on the network is able to use a “sniffer” program to view and capture data transmitted over the LAN. Consider implementing encryption software to protect confidential or sensitive data stored on the server or a workstation, or data being transmitted over the network. Encryption software protects data by making it unreadable. Encryption software uses an algorithm to scramble data. Only a person with the appropriate encryption key can unscramble the data to make it readable.



CIAO

Hub Management

Proper controls need to be implemented to appropriately manage an organization's hubs. Management tools can make this task easier. A current inventory should include all active hubs, the configuration for each, and a listing of ports and port settings.

Voice Operations

When security is an issue, an area that commonly lacks attention is the telecommunications networks that include all of the voice operations, PBXs, and other hardware and software. The focus typically is on modem lines, not voicemail systems, long distance capabilities, public access to phones, etc. Access controls are necessary to adequately protect voice operations from misuse and intrusion to more sensitive areas of an organization.

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



VAF Step 2.3 – Assess Areas of Control – Segregation of Duties

Description:

Policies, procedures, and an organizational structure established so that no one individual can control key aspects of computer-related operations or physical security and thereby conduct unauthorized actions or gain unauthorized access to assets, records, or other MEI resource elements.

Segregation of duties is defined as the process of segregating work responsibilities to ensure critical stages of a process are not under the control of a single individual. Segregation of duties is achieved by dividing responsibilities for critical process stages between two or more individuals or groups. Dividing duties allows for the activities of one group or individual to serve as a check on the activities of the other and reduces the probability of errors and wrongful acts going undetected.

Interviews and Data Gathering:

See Questionnaire in Appendix C.

To gather the information required in the questionnaire, the VAF team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated process and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the VAF team should meet with the staff responsible for setting policy and procedures and to identify those policies and procedures that are defined. The VAF team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify they are being followed.

Areas of Concern:

Key areas of concern during a vulnerability assessment involve the segregation of duties among major operating and programming activities, including duties performed by users, application programmers, and data center staff. The policies outlining the responsibilities of these groups and related individuals should be fully documented, communicated, and enforced. Effective supervision and management reviews are essential to ensuring policies and procedures are enforced. This holds especially true for procedures pertaining to the duties of computer operators, where segregation of duties alone does not ensure personnel only perform authorized activities.



CIAO

Control Objectives:

Conducting a vulnerability assessment on the effectiveness of segregating duties involves assessing the entity's efforts to perform each of the following critical elements: Policies; Access Controls to Enforce Segregation of Duties; and Operating Procedures, Supervision, and Review.

Policies

Policies should be defined and implemented to ensure incompatible duties are identified and segregated. In addition to segregating duties, these policies should clearly define employee duties and responsibilities.

Access Controls to Enforce Segregation of Duties

Management reviews must be performed to determine the effectiveness of established control techniques for segregating incompatible duties, in terms of both logical and physical access. These reviews should reveal whether or not control techniques are maintaining risks within acceptable levels.

Operating Procedures, Supervision, and Review

Formal operating procedures should be defined and implemented to provide guidance for the performance of personnel activities. Active supervision and review should be provided for all personnel to ensure procedures are being properly followed.

Interdependencies

When performing a vulnerability assessment of segregation of duties, it is important to consider the possible risks resulting from interdependencies. An example of risks resulting from interdependencies is the use of third party maintenance agreements by an outsourcing services firm.

Control Objective Topical Areas:

- Identify and segregate incompatible duties and establish policies
- Establish, implement, and enforce access controls to segregate duties appropriately
- Control personnel activities through formal operating procedures and supervision and review

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



VAF Step 2.4 – Assess Areas of Control – Continuity of Services and Operations

Description:

Controls to ensure that when unexpected events occur, critical business operations, including computer operations, continue without interruption or are promptly resumed and critical and sensitive data are protected.

Service continuity controls provide reasonable assurance that the elements supporting processes will be maintained. By taking steps to prevent and minimize potential damage and interruption, users of functional systems can rely on continuous service. Developing and documenting a comprehensive contingency plan creates procedures to resolve uncontrollable changes to systems. By maintaining and testing the contingency plan system, administrators can have confidence in the ability to provide continuous service.

The objectives of service continuity controls are to ensure that:

- the organization does not lose the capability to process, retrieve, and protect information maintained electronically,
- there are procedures in place to protect information resources and minimize the risk of unplanned interruptions,
- a plan exists to recover critical operations should interruptions occur, and
- recovery plans will work as intended, and are tested periodically in disaster simulation exercises.

If the objectives of the controls are met, the risk of loss of service is reduced. Adequate policies and procedures allow users to have confidence in the reliability and availability of the system they depend on.

Interviews and Data Gathering:

See Questionnaire in Appendix D.

To gather the information required in the questionnaire, the VAF team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated process and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals



CIAO

required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the VAF team should meet with the staff responsible for setting policy and procedures and to identify those policies and procedures that are defined. The VAF team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify they are being followed.

Areas of Concern:

Controls to ensure service continuity should address the entire range of potential disruptions. This includes the entire range of service interruptions from relatively minor interruptions to major disasters, such as fires or natural disasters. Service continuity controls may also include having procedures to reestablish operations at a remote location. Service continuity controls help prevent relatively minor interruptions from resulting in the loss or incorrect processing data, which could end in financial loss, expensive recovery efforts, or inaccurate financial or management information. For some operations, such as those involving health care or safety, system interruptions could also result in injuries or loss of life.

Control Objectives:

Business Continuity Plan

Business continuity plan (BCP) controls provide assurance that the BCP is adequate and addresses all areas necessary to support business processes. The BCP controls help ensure that critical resources are identified, emergency procedures are established, the BCP is continuously updated to address changes in structure or function, personnel is properly trained, and the plan is properly tested.

Resource Management

Resource management controls provide assurance that system capacity is maintained. Workload forecasting and system monitoring procedures help to ensure peak system performance. Scheduling policies reduce the impact of system maintenance on operations.

Contingency Plan

A contingency plan identifies procedures to account for loss of critical system processes or components. Contingency plan controls provide assurance that the contingency plan reflects current conditions, has been properly approved, addresses all components, and is properly tested.

Service Level Agreement Management



CIAO

Service level agreement controls provide assurance that frameworks for service level agreements have been defined. The agreements should cover such aspects as availability, reliability, performance, security, and levels of support. Service level agreement controls also provide for monitoring service and reviewing agreement and contracts.

Data Center Management

Data center management controls provide assurance that the data center facility is constructed and maintained so that service continuity disruptions are reduced. These controls address issues such as data center organization, location, and construction. Media library management provides assurance toward the control of physical data storage media.

Backup Management

Backup management controls provide assurance that backup policies and procedures are adequate. The controls ensure that the backup site is properly located, constructed, and maintained, that data and program procedures are properly implemented, and restoration strategies are adequate.

Alternative Site Management

Alternative site management controls provide assurance that alternative site procedures support all necessary business processes. These controls assess such components as site management policies, contracts and agreements, and alternate service arrangements.

Interdependency Awareness

Interdependency awareness controls provide assurance that management is aware of areas of dependency that are out of the organization's control. Interdependency awareness controls also ensure that management has considered constructing redundancy in areas that are critical to the continuity of critical business processes.



CIAO

Control Objective Topical Areas:

- Assess the criticality and sensitivity of computerized operations and identify supporting resources
- Prevent and minimize potential damage and interruption
- Develop a comprehensive contingency plan.
- Test contingency plan
- Problem & Performance Management

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



VAF Step 2.5 – Assess Areas of Control – Change Control & Life Cycle Management

Description:

Procedures and controls that prevent unauthorized programs or modifications to an existing program being implemented.

Change control and life cycle management (LCM) policies provide reasonable assurance that changes to applications will not interrupt the business process. Life cycle management policies provide direction toward software specifications, implementation, and testing. Change control policies provide assurance toward application and system modifications for in-house and commercial packages or patches. By instituting policies, procedures, and techniques, all program modifications are properly authorized, tested, and approved. In addition, access to and distribution of programs is carefully controlled.

The objectives of managing programs and program modifications are to ensure that:

- developers are deterred from modifying program code to provide a means of bypassing controls to gain access to sensitive data,
- program versions are controlled, limiting erroneous processing due to out of date versions; and
- proper testing takes place, limiting the implementation of non-functional programs.

If the objectives of the controls are met, the risk of incorrect modification is reduced and disruption of service avoided. Adequate implementation of control policies and procedures can have a large effect on the availability and reliability of both systems and applications.

Interviews and Data Gathering:

See Questionnaire in Appendix E.

To gather the information required in the questionnaire, the VAF team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated process and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the VAF team should meet with the staff



CIAO

responsible for setting policy and procedures and to identify those policies and procedures that are defined. The VAF team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify they are being followed.

Areas of Concern:

Life cycle management and change controls focus primarily on controlling the development process, and the update, maintenance, and modification of existing software systems. These controls are also effective in managing changes in systems under development.

Conducting a vulnerability assessment of life cycle management and change controls involves assessing current policies and procedures involving software development, changes, updates, and modifications. This may include examining policies involving software library management, change management, life cycle management, project management, and application management.

Control Objectives:

Change Management

Change management controls provide assurance that modification to software systems is conducted in a way that will limit impact on business processes. Change management policies include requiring authorization for software modification, controlling changes through testing to final approval, emergency change procedures, and control of the impact of changes on a functional system.

Life Cycle Management

Life cycle management controls provide assurance that software controlled properly from design to removal. LCM includes procedures for documentation, communication, implementation, and conversion.

Project Management

Project management controls provide assurance that software development projects will meet user and system requirements. Project management monitors and documents software development from design through production and implementation. Proper project management will ensure that developed software is complete and meets user requirements.



Application Acquisition, Management, and Maintenance

Application Acquisition, Management, and Maintenance controls provide assurance that processes are in place to control software distribution, version management, and documentation and manuals. Policies including distribution restriction, software version control, program library access and control, and maintenance of documents help ensure that appropriate software is accessible.

Quality and Assurance

Quality and assurance controls provide assurance that changes to software are validated and meet specifications. Quality and assurance policies include procedures for system, application, and operational tests, which contain processes to ensure that changes were implemented correctly and documented appropriately.

Interdependencies

Life cycle management and change controls are dependent upon many outside factors. An organization may be dependent upon a software vendor or third party developer to implement application changes. Organizations may also have a dependency on the quality of a commercial off-the-shelf product.

Control Objective Topical Areas:

- Authorization of Processing Features & Program Modifications
- Test and Approve all New and Revised Software
- Control Software Libraries

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



CIAO

VAF Step 2.6 – Assess Areas of Control – System Software

Description:

Controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system.

System software is a set of programs designed to operate and control the processing activities of computer equipment. System software helps control and coordinates the input, processing, output, and data storage associated with all of the applications that run on a system. Examples of system software include: operating system software, system utilities, program library systems, file maintenance software, security software, data communications systems, and database management systems.

Interviews and Data Gathering:

See Questionnaire in Appendix F.

To gather the information required in the questionnaire, the VAF team would review existing documentation and perform interviews. These two activities will provide the team insights as the team identifies and validates stated process and procedures and their current implementation within the organization. The interviews may serve as data gathering or as validation meetings.

At the beginning of the assessment, the VAF team should review the questionnaire and compile a list of documents required for review. The VAF team should also determine the individuals required for interviews. The policy staff may differ from the functional and technical staff responsible for the execution of policy. Initially, the VAF team should meet with the staff responsible for setting policy and procedures and to identify those policies and procedures that are defined. The VAF team should then follow up with the functional and technical staff responsible for carrying out the policy and procedures to verify they are being followed.

Areas of Concern:

It is essential that controls over access to and modification of system software are in place to ensure operating system-based security controls are not compromised and the system will not be impaired.

Conducting a vulnerability assessment of system software involves assessing the agency's efforts to perform each of the following critical elements: System Software Access Control, System Software Monitoring, and System Software Change Control.



CIAO

Control Objectives:

System Software Access Control

System software access control is the process of limiting and controlling system software access authorizations. Key to controlling access is the identification of all access paths and the implementation of controls to prevent or detect access for all paths.

System Software Monitoring

System software monitoring is performed to detect and track the use of system software utilities. System software monitoring, policies and techniques are implemented that govern the use and monitoring the use of system software utilities. Inappropriate or unusual activity that is detected through system software monitoring should be investigated and result in appropriate disciplinary actions.

System Software Change Control

System software change control is the process of controlling system software changes that result from installation and maintenance activities. All system software changes must be authorized, tested, and approved before implementation. Installation of system software must be fully documented and reviewed to ensure software change control can be maintained. System software maintenance must be performed in accordance with system software change control procedures.

Interdependencies

When performing a vulnerability assessment of system software it is important to consider the possible risks resulting from interdependencies. An example of system software risks resulting from interdependencies is the use of third party programming or maintenance resources by a system software vendor.

Control Objective Topical Areas:

- Limit Access to System Software
- Monitor Access & Use of System Software
- Control System Software Changes
- Limit Access to Data Center by System Software Personnel

Outcomes:

The identification of control weaknesses or vulnerabilities within one or more core processes.



V. VAF Step 3 – Analyze & Prioritize Vulnerabilities

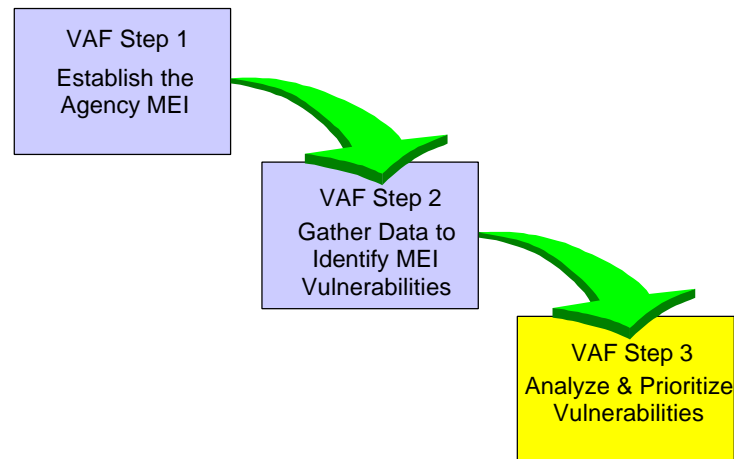


Figure 7. VAF Step 3

A. Objective

The objective of this step is to define and analyze the vulnerabilities identified in VAF Step 2 and MEI external dependencies from VAF Step 1, thereby enabling at least a first order of prioritization for purposes of remediation or minimization. This step will move the process from the vulnerability assessment phase into the first steps of the remediation planning process, with its accompanying funding estimates and timelines.

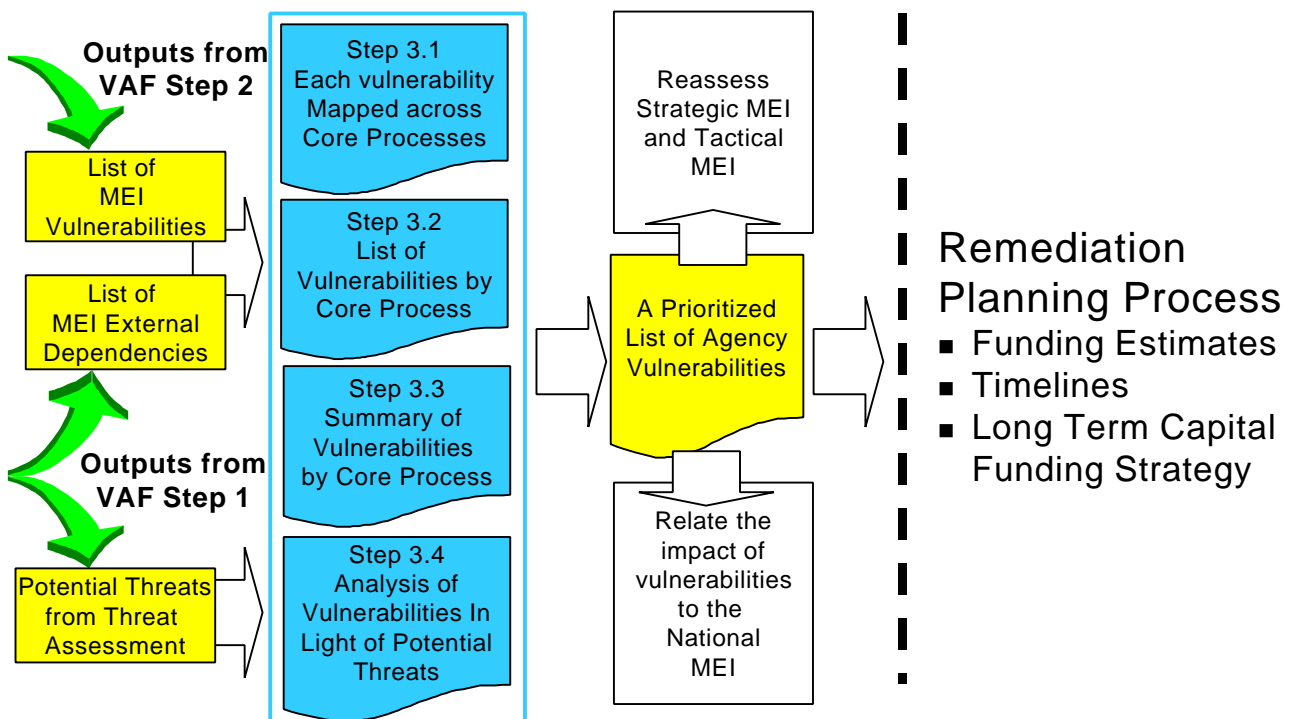


Figure 8. Activities in VAF Step 3



CIAO

B. Critical Success Factors

In order for this step to be successful, the following elements need to exist:

- ✓ Application and assignment of the appropriate, knowledgeable personnel to the process of mapping vulnerabilities to core processes
- ✓ A solid understanding of the relationship between core processes and critical agency missions
- ✓ An understanding of the relationship between agency MEI issues and the National MEI
- ✓ Access to outputs from Steps 1 and 2

C. Measurements in the four areas of compromise

For the areas of compromise, integrity, confidentiality and availability, the VAF team will assign a value of *Code Red*, *Code Amber* or *Code Green* to indicate the impact if the vulnerability is exploited.

However, for accountability, a *Code Red* is assigned if:

- a vulnerability is caused by a lack of accountability i.e. if ownership of the process, system or inputs/outputs is not clearly or appropriately defined; or
- a vulnerability is exploited and controls are not in place to warn those accountable.

This measurement will complement the review of the other areas of compromise and alert management to review the assignment of ownership and/or oversight to the particular process or system affected.

D. Outcomes

Each vulnerability will be examined to determine if it impacts more than one MEI core process and the level of impact (potential for loss) across the four areas of potential compromise. This will yield a cross cutting analysis of MEI impacts.

Second, vulnerabilities will be sorted by core process, presenting each identified vulnerability within that core process.

Third, a graphical summary of the number of vulnerabilities by core process will be generated.

Fourth, an analysis of the likelihood that a vulnerability will be exploited considering the potential threats to the agency will be performed.



E. Activities

VAF Step 3.1 – Document the Impact

First, for each vulnerability, document the impact on each core process and the interdependencies between and among core processes. The outcome is indicated by the *Code Red, Amber, Green* criteria defined in Step 1.4. The Figure 9 is a representative example of how this can be done.

Worksheet for Each Vulnerability or Control Weakness Noted				
Title:	Passwords			
Description:	System access passwords are not aged.			
Location:	Desktop PCs with network connections			
<u>Core Processes</u>	Integrity	Confidentiality	Accountability	Availability
Core Process 1	Green	Amber	Red	Green
Core Process 2	Amber	Red	Red	Amber
Core Process 3	Red	Amber	Green	Red
Core Process 4	Amber	Green	Red	Amber
Core Process "n"	Red	Green	Amber	Amber

Figure 9. Vulnerability Analysis Across MEI Core Processes

Objective: Evaluate each vulnerability and determine if the vulnerability impacts more than one MEI core process and the level of impact (potential for loss) across the four areas of compromise.

Outcome: Detailed analyses of vulnerabilities with crosscutting impacts in the MEI.



VAF Step 3.2 – Document the Vulnerabilities

Second, for each core process, document the vulnerabilities or control weaknesses noted and the impact in terms of each area of compromise. The outcome is again indicated by the *Code Red, Amber, Green* criteria defined in Step 1.4. The Figure 10 is a representative worksheet.

Example:

Worksheet for Each Core Process				
Title:	Core Process Name			
Description:	MEI Documentation			
Core Processes	Integrity	Confidentiality	Accountability	Availability
Vulnerability 1	Green	Amber	Red	Green
Vulnerability 2	Amber	Red	Red	Red
Vulnerability 3	Red	Amber	Green	Amber
Vulnerability 4	Amber	Red	Red	Green
Vulnerability 5	Red	Red	Amber	Green
Vulnerability "n"	Red	Green	Red	Amber

Figure 10. All Vulnerabilities Per Core Process

Objective: Evaluate the vulnerabilities associated with a single core process and determine the level of impact (potential for loss) across the four areas of compromise.

Outcome: Detailed analyses of the vulnerabilities with the highest impact in each core process.



VAF Step 3.3 – Summarize the Vulnerabilities

Third, graphically summarize the number of vulnerabilities in each priority category per core process. This time, the number of vulnerabilities in each category indicates the outcome. The following worksheet is a representative example of how this can be done.

Example:




Summary of Impact of Vulnerabilities			
Core Processes	Priority		
	 Code Red	 Code Amber	 Code Green
Core Process 1	12		20
Core Process 2	1	18	11
Core Process 3		27	
Core Process 4	43		15
Core Process 5	21	9	
Core Process "n"			

Figure 11. Total Vulnerabilities Per Core Process

Objective: Prepare a report of all the vulnerability impact assessments across core processes.

Outcome: Detailed analyses of those core processes with the greatest number of vulnerabilities in the *Code Red* and *Code Amber* categories.



VAF Step 3.4 – Evaluate the Vulnerabilities

Fourth, evaluate the vulnerabilities associated with a single core process and determine the likelihood that they may be exploited by the threats that were initially identified in the threat assessment, VAF Step 1.2. The following worksheet is a representative example of how this can be done.

Example: Worksheet of Potential Threat Impact				
Title: Core Process Name				
Description: Threat Assessment Documentation				
Potential Threats	Threat 1	Threat 2	Threat 3	Threat 4
Vulnerability 1	LOW	MEDIUM	HIGH	HIGH
Vulnerability 2	HIGH	MEDIUM	LOW	LOW
Vulnerability 3	MEDIUM	HIGH	LOW	LOW
Vulnerability 4	HIGH	MEDIUM	HIGH	MEDIUM
Vulnerability 5	LOW	LOW	MEDIUM	HIGH
Vulnerability "n"	LOW	HIGH	LOW	HIGH

Figure 12. Vulnerabilities & Threats

Objective: Evaluate the vulnerabilities associated with a single core process and determine the likelihood that they may be exploited by the threats that were initially identified in the threat assessment, VAF Step 1.2.

Outcome: Analysis of vulnerabilities in terms of the likelihood that they will be exploited in view of certain threat considerations.

Using these four metrics, the assessment team must now use its expert subjective judgement, based on agency cyber and physical security business process experience to assign priorities for vulnerability remediation or minimization. This rank order of vulnerabilities leads to three additional steps.



CIAO

First, the remediation priority list will form the basis for the remediation planning process. Funding estimates and timelines will flow from the examination of the specific vulnerabilities that need to be addressed.

Next, because infrastructure vulnerability assessment must become a cyclical, regularly repeated function, the outputs from Step 3 need to be fed back into the VAF process for reassessment of strategic and tactical MEI elements in the next vulnerability assessment period.

Finally, the impacts of the vulnerabilities identified, and the priorities for remediation or minimization, need to be compared to the national MEI and forwarded to the Critical Infrastructure Assurance Office for inclusion in the National Plan process.



VI. Next Steps

The VAF will result in the identification and prioritization of vulnerabilities for the organization. From this process, the organization will have established a list of vulnerabilities that require attention internally as well as those that affect the national critical infrastructure. Moving from execution of this framework, the organization should shift focus into the remediation phase.

Similar to the activities and procedures necessary to execute the VAF, to prepare for remediation, the organization must:

- Establish a management team or team(s) representing the areas to be affected and the functional expertise required (cyber and physical) to address high priority vulnerabilities.
- Identify budget requirements for establishing a remediation initiative and specific remediation activities
- Identify resource requirements – define government resources and contractor resources required
- Identify technical and physical impacts of remediation i.e. determine architectural considerations
- Establish a schedule and milestones to be achieved
- Involve the audit and QA component to ensure the effort is continuously monitored and on track.



VII. Glossary of Terms

Term	Definition
access controls	Procedures and controls that limit or detect access to MEI Resource Elements (People, Technology, Applications, Data and/or Facilities) thereby protecting these resources against loss of Integrity, Confidentiality Accountability and/or Availability.
accountability	The explicit assignment of responsibilities for oversight of areas of control to executives, managers, staff, owners, providers, and users of MEI Resource Elements.
ACL	Access Control Lists
ANSI	American National Standards Institute
applications	All application systems, internal and external, utilized in support of the core process.
areas of control	Collectively, controls consist of the policies, procedures, practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected. The control areas set out in the KPMG VAF process have been modified from GAO's FISCAM standards for auditing federal information systems. The FISCAM definitions of the control areas have been expanded for this VAF process to incorporate infrastructure vulnerability issues.
areas of potential compromise	These broad topical areas represent categories where losses can occur that will impact both a department or agency's MEI and its ability to conduct core missions.
ARS	Automatic Route Selection
availability	The ability to have access to MEI Resource Elements when required by the mission and core supporting process(s), both now and in the future. It also concerns the safeguarding of those resources and associated capabilities.
BCP	Business continuity plan
CCTV	Closed Circuit Television
CDR	Call Detail Report
CEO	Chief Executive Officer
CFO	Chief Financial Officer



CIAO

Term	Definition
Change control & life cycle management	Procedures and controls that prevent unauthorized programs or modifications to an existing program from being implemented.
CIAO	Chief Infrastructure Assurance Officer; also, Critical Infrastructure Assurance Office
CICG	Critical Infrastructure Coordination Group
CIO	Chief Information Officer
CMS	Call Management System
CO/DO	Central Office/Direct Outdial
COB	Continuity of Business
COBIT™	Control Objectives for Information Technology
<i>Code Amber</i>	Significantly debilitate the ability of the Agency to fulfill its mission, critical national security or national economic security functions or provide continuity of government services.
<i>Code Green</i>	No appreciable impact on agency missions.
<i>Code Red</i>	Prevent the Agency from fulfilling its mission, critical national security or national economic security functions or from providing continuity of core government services. From the perspective of an attacker, this would constitute a “Kill.”
confidentiality	The protection of sensitive information from unauthorized disclosure and sensitive facilities from physical, technical or electronic penetration or exploitation.
CONOPS	Concept of Operations
continuity of services & operations	Controls to ensure that, when unexpected events occur, departmental/agency MEI services and operations, including computer operations, continue without interruption or are promptly resumed and critical and sensitive data are protected through adequate contingency and business recovery plans and exercises.
control objectives	A statement of the desired result or purpose to be achieved by implementing control procedures in a particular IT activity.
COO	Chief Operations Officer
COOP	Continuity of Operations



CIAO

Term	Definition
COR	Class of Restriction
COS	Class of Service
data	All data (electronic and hard copy) and information required to support the core process. This includes numbers, characters, images or other method of recording, in a form which can be assessed by a human or (especially) input into a computer, stored and processed there, or transmitted on some digital/communication's channel.
DBMS	Database Management System
DBU	Dial Backup
DD	Data Dictionary
delete access	the ability to erase or remove data or programs
DES	Data Encryption Standard
DISA	Direct Inward System Access
entity-wide security	Planning and management that provides a framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of the entity's physical and cyber security controls.
execute access	the ability to execute a software program
facilities	All facilities required to support the core processes, including the resources to house and support information technology resources, and the other resource elements defined above.
FEMA	Federal Emergency Management Agency
FIPS	Federal Information Processing Standard
FISCAM	Federal Information Systems Control Audit Manual
FMFIA	Federal Manager's Financial Integrity Act
FRL	Facility Restriction Level
FTP	File Transfer Protocol
GAO	General Accounting Office
HR	Human Resources



CIAO

Term	Definition
integrity	The accuracy, completeness and reliable transmission and reception of information and its validity in accordance with business values and expectations; the adequacy and reliability of processes assuring personnel selection, access and safety; and the adequacy and reliability of processes assuring only authorized access to, and safety of, physical facilities.
IPL	Initial Program Load
IS	Information System
ISACF	Information Systems Audit and Control Foundation
ISP	Internet Service Provider
IT	Information Technology
LAN	Local Area Network
LCM	Life Cycle Management
life cycle management	See change control and life cycle management
MAC	Moves Adds Changes
MEI	Minimum Essential Infrastructure
MEI resource elements	As previously discussed, these are the broad categories of resources, all or portions of which constitute the minimal essential infrastructure necessary for a department, agency or organization to conduct its core mission(s). These resource elements are very similar to, but modified somewhat from, the COBIT™ framework used by ISACF. The definitions have been expanded to incorporate physical infrastructure vulnerability areas.
MEP	Mission Essential Processes
merge access	the ability to combine data from two separate sources
NMS	Network Management Systems
OMB	Office of Management and Budget
PBX	Public Branch Exchange
PCCIP	Presidential Commission on Critical Infrastructure Protection
PCM	Procedures Control Manual
PDD	Presidential Decision Directive



CIAO

Term	Definition
people	Staff, management, and executives necessary to plan, organize, acquire, deliver, support, and monitor mission related services, information systems, and facilities. This includes groups and individuals external to the organization involved in the fulfillment of the organization's mission. Security management personnel should also be included.
PIN	Personal Identification Number
questions on controls	The policies and procedures and practices and organizational structures designed to provide reasonable assurance that business objectives will be achieved and that undesired events will be prevented or detected and corrected.
read access	the ability to look at and copy data or a software program
segregation of duties	Policies, procedures, and an organizational structure established so that one individual cannot control key aspects of physical and/or computer-related operations and thereby conduct unauthorized actions or gain unauthorized access to MEI Resource Elements.
SLA	Service Level Agreement
system software	Controls that limit and monitor access to the powerful programs and sensitive files that (1) control the computer hardware and (2) secure applications supported by the system.
TAC	Trunk Access <i>Codes</i>
technology	All hardware and software, connectivity, countermeasures and/or safeguards that are utilized in support of the core process.
topical areas	A grouping of related control objectives.
TSO	Time Share Option
update access	the ability to change data or a software program
UPS	Uninterrupted Power Supply
VAF	Vulnerability Assessment Plan
VDN	Vector Directory Number
VRU	Voice Response Unit
WAN	Wide Area Network



VIII. Primary Source Documents

Davis, Beth. “Eye on the Spies.” *InformationWeek/Ernst & Young Security Survey* (September 1997).

COBIT, 2nd Edition. Information Systems Audit and Control Foundation. *Control Objectives for Information and Related Technology*. Rolling Meadows, Illinois, 1998.

Gartner Group Report. Information Security Strategies. *Security Vulnerabilities in Emerging Technologies* (October 1995).

Gartner Group Report. Information Security Strategies. *Enterprise Client/Server Security - An Illusion of Grandeur* (November 1995).

Gartner Group Report. Information Security Strategies. *Strategic Analysis Report: Internet Security for the Enterprise* (September 1995).

Gartner Group Report. Information Security Strategies. *Security: The Never-Ending Challenge* (September 1995).

Gartner Group Report. Information Security Strategies. *ISS Internet Scanner* (July 1996).

Gartner Group Report. Information Security Strategies. *1997 Information Security Key Issues* (March 1997).

Gartner Group Report. Information Security Strategies, *The Internetworking Security Scenario: 1998 to 2001* (September 1997).

Gartner Group Report. Information Security Strategies. *Information Warfare* (December 1996).

Gartner Group Report. Internet Strategies. *Best Practices for Web Site Security* (January 1997).

Koprowski, Gene. “Hacking the Power Grid.” *Information Week Online* (June 1998).

National Research Council. Commission on Physical Sciences, Mathematics, and Applications. Computer Science and Telecommunications Board. Committee on Maintaining Privacy and Security in Health Care Applications of the National Information Infrastructure. *Protecting Electronic Health Information*. Washington, D.C., 1997.



National Security Telecommunications Advisory Committee. Information Assurance Task Force. *Electric Power Risk Assessment Executive Summary of the Electric Power Information Assurance Risk Assessment Report*. Washington, D.C., 1997.

Neumann, Peter G. “Security Risks in the Emerging Infrastructure.” *Congressional Testimony* (August 1997).

Neumann, Peter G. “Computer-Related Infrastructure Risks for Federal Agencies.” *Testimony for the U.S. Senate Committee on Governmental Affairs* (May 1998).

New York Law School. Communications Media Center. *Computer Crime Survey*. New York, 1997.

Polk, Timothy. *Automated Tools for Testing Computer System Vulnerability*. 1992.

Rathmell, Andrew, Lorenzo Valeri and John Gearson. “The Threat from Sub-State Groups: an Interdisciplinary Approach.” Third International Symposium on Command and Control Research and Technology, Institute for National Strategic Studies, National Defense University, June 1997.

U.S. Department of Commerce. National Institute of Standards and Technology. *Generally Accepted Principles and Practices for Securing Information Technology Systems*. Washington, D.C., 1996.

U.S. Department of Commerce. National Institute of Standards and Technology. *An Introduction to Computer Security: The NIST Handbook*. Washington, D.C.

U.S. Department of Commerce. President’s Commission on Critical Infrastructure Protection. *Critical Foundations - Protecting America’s Infrastructures*, Washington, D.C., October 1996.

U.S. Department of Commerce. President’s Commission on Critical Infrastructure Protection. *Critical Foundations Protecting America’s Infrastructures, The Report of the President’s Commission on Critical Infrastructure Protection*. Washington, D.C., 1997.

U.S. Department of Defense. Protection of DoD Personnel and Activities Against Acts of Terrorism and Political Turbulence, Washington DC February 1993

U.S. Department of Energy. Safeguards and Security Central Training Academy, *Vulnerability Assessment Fundamentals*, Washington DC May 1994

U.S. Department of Justice. *Vulnerability Assessment of Federal Facilities*, Washington, DC June 1995



CIAO

U.S. General Accounting Office. GAO Executive Guide. *Information Security Management, Learning from Leading Organizations.* Washington, D.C., May 1998.

U.S. General Accounting Office. GAO Federal Information Systems Control Audit Manual (FISCAM). Washington, D.C., Draft, Summer 1998.

U.S. General Accounting Office. GAO Information Security. *Report to Congressional Requesters: Opportunities for Improved OMB Oversight of Agency Practices.* Washington, D.C., September 1996.

U.S. General Accounting Office. General Services Administration. *Many Building Security Upgrades Made But Problems Have Hindered Program Implementation.* Washington D.C., June 1998.



CIAO

Web Sites:

Australian CERT	www.auscert.org.au/
NIST	www.nist.gov/
CERT Coordination Center	www.cert.org/
Risks Forum Digest	catless.ncl.ac.uk/Risks
Naval Surface Warfare Center Info Sec	www.nswc.navy.mil/ISSEC/
International Computer Security Assn	www.ncsa.com
Computer Crimes & Investigation Center	www.ovnet.com/~dckinder/crime
COAST	www.cs.purdue.edu/coast/
Defense Information Systems Agency	www.disa.mil
CIAC	www.ciac.llnl.gov/ciac/
National Security Institute	www.nsi.org
GartnerGroup	www.gartner.com
NSA	www.nsa.gov



CIAO

**Appendix A:
Entity-Wide Security**

Control Objectives	Control Technique	Compliance Procedures
Organizational Management		
1.1 Maintain a positive information control environment.	Does Management create a framework and an awareness program fostering a positive control environment throughout the entire organization by addressing aspects such as: integrity, ethical values and competence of the people; management philosophy and operating style; and accountability, attention and direction provided by the board of directors?	Interview CEO, COO, CFO, CIO, Security Officer, IS Senior Management, IS planning/steering committee members. Review related policies and procedures. Review Senior Management roles and responsibilities. Review objectives and long/short range plans.
1.2 Periodically assess risks	Are independent risk assessments performed and documented on a regular basis?	Review risk assessment policies.
	Is a security plan documented and approved? Has independent advice and comment been solicited on the plan before it's implementation?	Review the most recent high-level risk assessment.
	Does the risk assessment consider data sensitivity and integrity and the range of risks to the entity's systems and data?	Review the objectivity of personnel who performed and reviewed the assessment.
1.3 A policy on intellectual property, privacy and data flow exists.	Does management provide and implement a written policy on intellectual property rights covering in-house as well as contract-developed software?	Review related policies.
	Does management ensure compliance with privacy, intellectual property, transborder data flow and cryptographic regulations applicable to the information technology practices of the organization?	Interview Senior Management. Review external requirements.



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
1.4 Proactive Audit Involvement	Does Information Technology management seek audit involvement in a proactive manner before finalizing information technology service solutions?	Interview IT Senior Management.
	Do the managers' whose missions they support accredit major systems and applications?	Review accreditation statements.
1.5 Management ensures that corrective actions are effectively implemented	Does top management initiate prompt action to correct deficiencies?	Review documentation related to corrective actions.
	Are corrective actions tested after they have been implemented and monitored on a continuing basis?	Review the status of prior year audit recommendations and determine if implemented corrective actions have been tested. Review recent FMFIA reports.



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
Security Program Plan		
2.1 A security plan is documented and approved.	<p>Is a security program plan documented?</p> <p>If so, does it cover the following:</p> <ul style="list-style-type: none">■ covers all major facilities and operations,■ has been approved by key affected parties, and■ covers the topics prescribed by OMB Circular A-130 (general support systems/major applications) <p>Rules of the system/Application rules</p> <p>Training/Specialized training</p> <p>Personnel controls/Personnel security</p> <p>Incident response capability/</p> <p>Continuity of support/Contingency planning</p> <p>Technical security/Technical controls</p> <p>System interconnection/Information sharing</p> <p>Public access controls</p>	<p>Review the security plan</p> <p>Determine whether the plan covers the topics prescribed by OMB Circular A-130.</p>
2.2 The plan is kept current	<p>Is the plan reviewed periodically and adjusted to reflect current conditions and risks?</p>	<p>Review the security plan and any related documentation indicating that it has been reviewed and updated, and is current.</p>



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
2.3 Compliance with Policies, Procedures and Standards	<p>Does management ensure that appropriate procedures are in place to determine whether personnel understand the implemented policies and procedures, and that the policies and procedures are being followed?</p> <p>Are compliance procedures for ethical, security and internal control standards set by top management and promoted by example?</p>	<p>Interview Senior Management.</p> <p>Review policies and procedures.</p> <p>Interview staff.</p>
	<p>Do your security plans adequately address regulations on classified systems?</p>	<p>Review security plan and any related documentation indicating that regulations on classified systems are addressed.</p>
Security Management		
3.1 Establish a security management structure, and clearly assign security responsibilities	<p>Does the security program plan establish a security management structure with adequate independence, authority, and expertise?</p>	<p>Review the security plan, and the entity's organization chart.</p> <p>Interview security management staff.</p>
3.2 A security management structure has been established	<p>Has an information systems security manager been appointed at an overall level and at appropriate subordinate levels?</p>	<p>Review pertinent organization charts and job descriptions.</p> <p>Interview the security manager.</p>



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
3.3 Information security responsibilities are clearly assigned	Does the security plan clearly identify who owns computer-related resources and who is responsible for managing access to computer resources? Are security responsibilities and expected behaviors clearly defined for (1) information resource owners and users, (2) information resources management and data processing personnel, (3) senior management, and (4) security administrators?	Review the security plan.
3.4 Owners and users are aware of security policies	Has an ongoing security awareness program been implemented? Does it include first time training for all new employees, contractors, and users, and periodic refresher training thereafter? Are security policies distributed to all affected personnel, including system/application rules and expected behaviors?	Review documentation supporting or evaluating the awareness program. Observe a security briefing. Interview data owners and system users. Review memos, electronic mail files or other policy distribution mechanisms. Review personnel files to test whether security awareness statements are current. Interview personnel to determine if they are aware of their security-related responsibilities.



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
3.5 An incident response capability has been implemented	Has an incident response capability been implemented?	<p>Interview security manager, response team members, and system users.</p> <p>Review documentation supporting incident handling activities.</p> <p>Determine qualifications of response team members.</p> <p><i>(Note: See also Critical Element on monitoring access and security violations.)</i></p>
Human Resources Policies		
4.1 Hiring, transfer, termination, and performance policies address security	Does management implement and regularly assess the needed processes to ensure that personnel recruiting and promotion practices are based on objective criteria and consider education, experience and responsibility?	<p>Interview Senior Management.</p> <p>Review relevant personnel processes.</p>
	For prospective employees, are references contacted and background checks performed?	<p>Review hiring policies.</p> <p>For a selection of recent hires, inspect personnel records and determine whether references have been contacted and background checks have been performed.</p>
	Does Management of the information services function ensure that their personnel are subjected to security clearance before they are hired, transferred or promoted, depending on the sensitivity of the position?	<p>Review hiring, transfer, and promotion policies.</p> <p>For a selection of hired, transferred, and promoted employees, inspect personnel records and determine whether appropriate security clearances have been performed.</p>



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
	Are confidentiality agreements required for employees and contractors assigned to work with confidential information?	Review policies on confidentiality agreements. For a selection of such users, determine whether confidentiality agreements are on file.
	Are regularly scheduled vacations exceeding several days required? If so, is the individual's work is temporarily reassigned?	Review vacation policies. Inspect personnel records to identify individuals who have not taken vacation or sick leave in the past year. Determine who performed vacationing employee's work during vacation.
	Are regular job or shift rotations required?	Review job rotation policies. Review staff assignment records and determine whether job and shift rotations occur.
	Do termination and transfer procedures include <ul style="list-style-type: none">■ exit interview procedures;■ return of property, keys, identification cards, passes, etc.;■ notification to security management of terminations and prompt revocation of IDs and passwords;■ immediately escorting terminated employees out of the entity's facilities; and■ a period during which non-disclosure requirements remain in effect	Review pertinent policies and procedures. For a selection of terminated or transferred employees, examine documentation showing compliance with policies. Compare a system-generated list of users to a list of active employees obtained from personnel to determine if IDs and passwords for terminated employees exist.



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
4.2 Employees have adequate training and expertise	Are skill needs accurately identified and included in job descriptions, and employees meet these requirements?	Review job descriptions for security management personnel, and for a selection of other personnel. For a selection of employees, compare personnel records on education and experience with job descriptions.
	Has a training program has been developed?	Review training program documentation.
	Does management provide for sufficient cross-training or back up of identified key personnel to address when that key personnel is not available?	Review training program documentation.
	Are employee training and professional development documented and monitored?	Review training records and related documentation showing whether such records are monitored and whether employees are receiving the appropriate training.
Outsourcing		
5. Third-Party Management	Does management ensure that all third-party providers' services are properly identified and that the technical and organizational interfaces with suppliers are documented?	Review vendor selection policies. Interview Senior Management. Review documentation.
	Does management define specific procedures to ensure that for each relationship with a third-party service provider a formal contract is defined and agreed upon?	Review contracts. Review procedures.



ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
	Does management ensure that, before selection, potential third parties are properly qualified through an assessment of their capability to deliver the required service (due diligence)?	Review selection policies. Review third-party assessment procedures.
	Are specific organizational procedures defined that ensure the contract between the facilities management provider and the organization is based on required processing levels, security, monitoring and contingency requirements, and other stipulations as appropriate?	Review relevant procedures. Review contracts. Review third-party requirements.
	With regard to relationships with third-party service providers, does management ensure that security agreements (e.g., non-disclosure agreements) are identified and explicitly stated and agreed to, and conform to universal business standards in accordance with legal and regulatory requirements, including liabilities?	Review contracts. Review legal and regulatory requirements.
	Does a continuous process for monitoring third-party adherence to contract agreements exist?	Review relevant policies and procedures.
Electronic Commerce		
6. Electronic Commerce	Does management ensure that formal contracts are in place establishing agreement between trading partners on communication processes and on standards for transaction message security and data storage?	Review applicable contracts. Interview Senior Management.



CIAO

ENTITY-WIDE SECURITY

Control Objectives	Control Technique	Compliance Procedures
	When trading on the Internet, does management enforce adequate controls to ensure compliance with local laws and customs on a worldwide basis?	Review relevant laws and customs. Review policies and procedures. Interview Senior Management.
	Do policies exist regarding authentication using certificate authorities?	Review policies and procedures. Interview Senior Management.

Appendix B:



Appendix B: Access Controls

Control Objectives	Control Technique	Compliance Procedures
Data Types		
1.1 Resource types and related criteria have been established	Have types and criteria been established and communicated to resource owners?	Review policies and procedures. Interview resource owners.
1.2 Owners have classified resources	Are resources classified based on risk assessments? Are classifications documented and approved by an appropriate senior official? Are they periodically reviewed?	Review resource classification documentation and compare to risk assessments. Discuss any discrepancies with appropriate officials.
1.3 Protection of Sensitive Information During Transmission and Transport	Management should ensure that adequate protection of sensitive information is provided during transmission and transport against unauthorized access, modification and misaddressing.	Review policies to determine if guidance is given reference transmission of sensitive information. Review and observe individuals to determine if compliant.
Access Control Lists (ACL)		
2.1 Resource owners have identified authorized users and their access authorized.	Are access authorizations documented on standard forms and maintained on file, approved by senior managers, and securely transferred to security managers?	Review pertinent written policies and procedures. For a selection of users (both application user and IS personnel), review access authorization documentation.
	Do owners periodically review access authorization listings and determine whether they remain appropriate?	Interview and review documentation. Determine whether inappropriate access is removed in a timely manner.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
2.2 User Account Management	Do procedures include the use of an access request form for the creation, maintenance, and deletion of User IDs, and does the form minimally require both the requester and the requestor's supervisor to sign the form?	Review user account management procedures. Review a sample of the access request forms and verify that the requester and supervisor have signed off on the forms.
	If the user is requesting access to resources that belong to another system/resource owner, is that system/resource owner <i>also required</i> to approve the request in addition to the user's supervisor? Does the process include a mechanism for the Security Administrator to validate that the appropriate parties have signed the access request?	Review a sample of the access request forms and verify for resources, which belong to another system/resource or that there are appropriate signatures to verify the granting of access. Verify that the correct Product Sponsor is granting approvals, via the list of applications and data from above section. Verify that there is a mechanism for Security Administrator validation.
	Do access request forms contain sufficient detail to determine exactly what type of access is being requested?	Sample access request forms and verify that the appropriate information is present to judge whether all requests are proper and that unique tracking numbers are assigned to each form.
	Are unique tracking numbers assigned to each request form?	Sample access request forms.
	Are rejected requests logged and returned to users with a stated reason?	Review request logs to verify rejected requests are being logged.
	Is there a monthly process and procedure to identify, remove or deactivate unused accounts from the system, according to policy requirements (60 days disable, 90 days delete)?	Check that a process has been established and documented for the removal of no-longer required and unused IDs from the system.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is security notified immediately when system users are terminated or transferred?	Obtain a list of recently terminated employees from Personnel and, for a selection, determine whether system access was promptly terminated.
	Is the number of users who can dial into the system from remote locations limited and justification for such access documented and approved by owners?	Review authorization and justification for a selection of users with dial-up access.
	Do security managers review access authorizations and discuss any questionable authorizations with resource owners?	Interview security managers, and review documentation provided to them.
	Are all changes to security profiles by security managers automatically logged and periodically reviewed by management independent of the security function?	Review a selection of recent profile changes and activity logs.
2.3 Emergency and temporary access authorization is controlled	<p>Are emergency and temporary access authorizations:</p> <ul style="list-style-type: none">■ documented on standard forms and maintained on file,■ approved by appropriate managers,■ securely communicated to the security function;■ automatically terminated after a predetermined period?	<p>Review pertinent policies and procedures.</p> <p>Compare a selection of both expired and active temporary and emergency authorizations (obtained from the authorizing parties) with a system-generated list of authorized users.</p> <p>Determine the appropriateness of access documentation and approvals, and the timeliness of terminating access authorization when no longer needed.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
2.4 Emergency Access Control	Do procedures exist that govern the granting of emergency or sensitive access?	Review procedures for emergency access control. Verify procedures are implemented in audit trails, and security logs.
	Has the definition of an emergency ID been defined, as to whom, why, and when it is needed? Are system activities and events performed by the emergency ID monitored via system generated audit trails?	Verify that the ID is only used in an emergency by the monitoring of its use and reason for use. View a system log showing its use, and those that use it, have appropriate authorizations.
2.5 Owners determine disposition and sharing of data.	Are standard forms used to document approval for archiving, deleting, or sharing data files?	Examine standard approval forms. Interview data owners.
	Are agreements documented regarding how files are to be protected prior to sharing data or programs with other entities?	Examine documents authorizing file sharing and file sharing agreements.
Physical Controls		
3.1 Facility Categories	Based on factors such as size, number of employees, use, and required access to the public how would you categorize your facility?	Categorize your facility.
	Is your facility a federal building?	Review documentation of facility
	If yes, what level of contact does your facility have with the general public?	Review levels of contact with the public.
	Do you own or lease your facility?	Review legal documentation regarding use of facility.
	Does your facility support a critical national security mission?	Review mission of organization occupying facility.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.2 Construction	What year was construction of facility completed?	Research and document the details of the facility's construction. Consult blueprints and current occupancy statistics if applicable.
	What material(s) were used to construct the facility's exterior (brick, block, concrete, metal panels or glass exterior)?	Review blueprints and building specs.
	What percentage of the external coverage is composed of special glass (Mylar Film, Ballistic Treatment, Polymer, or Wire Reinforced)?	Review blueprints and building specs.
	What is the total square footage of the facility (include office, storage and circulation space)?	Review blueprints and building specs.
	What is the total number of floors above ground?	Review blueprints and building specs.
	What is the total number of floors below ground (include underground parking if applicable)?	Review blueprints and building specs.
	What is the total number of occupants?	Interview facilities manager and human resources. Consult blueprints for number of offices/workspaces.
	What is the total number of daily visitors (estimate)?	Interview lobby security guard. Review visitor sign-in documentation.
3.3 Day Care Center	Is there a day care center on-site?	Review location and surroundings of day care center if part of facility.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	If yes, what is the location within the facility (interior space, exterior space above ground, below ground)?	Review blueprints and building specs.
	What is the point of main entry to the day care center (interior door, exterior door)?	Review blueprints and building specs.
	Is there an outside playground area?	Review blueprints, exterior surroundings and building specs.
3.4 Interior Security	Do you have procedures for securing the control of employee/visitor identification, utilities, and occupant emergency plans and day care centers?	Review procedures for securing access to the interior of the facility.
3.5 Security Planning	Have intelligence sharing, training, tenant assignment, administrative procedures, construction/renovation been considered and/or implemented at your facility?	Review security-planning procedures.
3.6 Fragmented Facilities	Has consideration been given to shared space and/or satellite offices?	Determine whether facility is fragmented.
3.7 Public Access	What is the distance in yards from the nearest public street?	Review details of public access to facility.
	What is the distance in yards from the building to the nearest public on-street parking?	Consult city planning. Review documentation.
	What is the distance in yards from the building to the nearest public parking lot?	Consult city planning. Review documentation.
	Are there public parks, plazas or other public areas immediately adjacent to the building?	Consult city planning. Review documentation.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are there any commercial businesses (e.g. restaurants, drug stores, and banks) with uncontrolled external access in the building (Yes/No)?	Consult city planning. Review documentation.
3.8 On-Site Parking	Is there parking on the property?	Review blueprints and building specs. Review parking options and security for each.
	If underground, is access controlled?	Consult alarm systems documentation.
	What type of control (security guard, automated/electronic control, vehicle barriers)?	Consult alarm systems documentation and security plan.
	Is public parking available?	Review blueprints and building specs.
3.9 Perimeter Security	Have you considered parking, closed circuit television monitoring, lighting and physical barriers in your security plan?	Evaluate options and procedures for securing the perimeter of the facility.
	Is there an alarm system?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	If yes, does the alarm system cover doors and windows?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	Who monitors the system?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is the alarm system operational?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	Is the facility electronically monitored (CCTV)?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	If yes, is it local, remote or video recording?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	Is CCTV operational?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	Is there an exterior roving patrol?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	If yes, who performs this task?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	Is exterior roving patrol operational?	Review systems that control perimeter security, including alarm systems, monitors, CCTV, exterior roving patrol, etc.
	What materials constitute the exterior barriers (concrete, fences, planters, pillars, and vehicle gate controls)?	Identify documentation that indicates the materials used in the construction of the exterior barriers.
	Are exterior barriers operational?	Test the exterior barriers.
	Are dumpsters in a Secured Area?	Review location of the dumpsters.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.10 Entry Security	What is the total number of entrances with x-ray and metal detector? (Indicate whether only visitors are screened or if everyone entering the building is screened.)	Review security of entrances.
	What is the total number of entrances with metal detector only? (Indicate whether only visitors are screened or if everyone entering the building is screened.)	Review documentation indicating security devices installed on or around entrances.
	What is the total number of entrances with security system access (e.g., Key Card)	Review documentation indicating security devices installed on or around entrances.
	What is the total number of entrances with security guard? (Indicate whether visitors must sign in.)	Review documentation indicating security personnel located on or around entrances.
	What is the total number of entrances without security?	Review documentation indicating security devices/people installed/located on or around entrances.
	Have you secured receiving/shipping, access control and entrances/exits?	Review security of all entries to facility. Review documentation indicating a lapse in security.
3.11 Security Screening	Are magnetometers and/or X-rays used in this facility at other than public entrances (e.g. at the entrance to a specific agency or office)? Yes/No	Determine levels and locations of security screening and review effectiveness.
	If so, who is screened? Everyone, including employees and tenants? Visitors only?	Determine levels and locations of security screening and review effectiveness.
	Does the facility have a screening process for mail?	Review documentation indicating that a screening process for mail exists.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	If so, where does the process take place (public entrance, mailroom, garage/loading dock, other)?	Review documentation that describes the procedure for mail screening.
	Does the facility have a screening process for deliveries?	Review documentation indicating that a screening process for deliveries exists.
	If so, where does the process take place (public entrance, mailroom, garage/loading dock, other)?	Review documentation that describes the procedure for delivery screening.
	Is maintenance and custodial staff required to enter the building through a secured area?	Review documentation indicating procedure for custodial staff entry.
3.12 Bomb Threats	Does the facility have an occupant emergency plan?	Review historical and current procedures and plans for action in case of a bomb threat.
	Has this building received a bomb threat in the past five years?	Review documentation indicating that a bomb threat was received.
	If so, how many bomb threats has the building received?	Review documentation indicating that a bomb threat was received.
	How many of the bomb threats have resulted in a building evacuation?	Review documentation indicating that a bomb threat was received and how the crisis was resolved.
3.13 Hours of Operation	Excluding unusual overtime situations, how many days of the week is this facility open to employees? The public?	Document hours of operation and identify personnel with access to the facility.
	How many hours is this facility open to employees? To the public?	Document hours of operation and identify personnel with access to the facility.
3.14 Security Systems	Are Duress Alarms present in the facility (perimeter/interior)?	Review documentation indicating location and type of security systems on-site.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is CCTV present in the facility (perimeter/interior)?	Review documentation indicating location and type of security systems on-site.
	Is there a remote monitoring facility located on-site?	Review documentation indicating location and type of security systems on-site.
	Is there a security console on-site?	Review documentation indicating location and type of security systems on-site.
	If so, how many hours a day is the security console monitored?	Review documentation indicating location and type of security systems on-site.
	Is emergency power available (generator, battery operated lighting)?	Review documentation indicating location and type of security systems on-site.
	Is there a fire detection/suppression system present (complete, partial, none)?	Review documentation indicating location and type of security systems on-site.
3.15 Protection of Utilities	Are there exterior propane fuel tanks?	Review procedures for protecting utilities.
	Are they protected?	Review architectural plans and city documentation.
	Is the water supply to the building protected?	Review architectural plans and city documentation.
	Is the main unit of the air/ventilation system accessible to the public?	Review architectural plans and city documentation.
	Is the wire closet locked?	Review architectural plans and city documentation.
	Is there utility access locked?	Review architectural plans and city documentation.
	Is there exterior access to the electric service?	Review architectural plans and city documentation.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is there exterior access to the gas service?	Review architectural plans and city documentation.
	Is there exterior access to the water service?	Review architectural plans and city documentation.
	Is there exterior access to the telephone service?	Review architectural plans and city documentation.
	Is there exterior access to other heating sources?	Review architectural plans and city documentation.
	Is fuel stored within the building?	Review architectural plans and city documentation.
3.16 Electronic Monitoring	Are the lobbies monitored by electronic means?	Review location and type of electronic monitoring systems within and around facility.
	Are secured corridors monitored by electronic means?	Review documentation from electric monitoring installation.
	Are courtrooms monitored by electronic means?	Review documentation from electric monitoring installation.
	Is parking monitored by electronic means?	Review documentation from electric monitoring installation.
	Are cellblocks monitored by electronic means?	Review documentation from electric monitoring installation.
	Is prisoner handling monitored by electronic means?	Review documentation from electric monitoring installation.
	Are office doors monitored by electronic means?	Review documentation from electric monitoring installation.
	Are stairwells monitored by electronic means?	Review documentation from electric monitoring installation.
	Is the security screening post monitored by electronic means?	Review documentation from electric monitoring installation.
	Is the interior security patrol monitored by electronic means?	Review documentation from electric monitoring installation.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is the building perimeter monitored by electronic means?	Review documentation from electric monitoring installation.
	Are entrances monitored by electronic means?	Review documentation from electric monitoring installation.
	Are garages monitored by electronic means?	Review documentation from electric monitoring installation.
3.17 The Security Force	What are the total number of federal police and/or guards and number of hours of coverage?	Review number, level and effectiveness of security forces on-site.
	What equipment has been issued to guards (firearm, handcuffs, baton, gas, 2-way radio, none)?	Review documentation indicating type of equipment issued to guards.
	Is the present security force strength and composition commensurate with the degree of security protection required by regulation or organizational definition?	Review documentation indicating strength and composition of security force. Compare documentation to security force regulations and organizational definition.
	Are all security posts fixed and mobile provided with security force orders?	Review documentation defining security force orders sent to all security posts.
	Are security force orders reviewed by the security officer for currency at least monthly?	Consult documentation from security force order reviews.
	Are security force personnel inspected by a supervisor prior to being posted?	Review documentation regarding security guard inspection. Interview supervisor for security force personnel.
	Do supervisors inspect each post/patrol/activity at least twice per shift?	Review documentation regarding security guard inspection. Interview supervisor for security force personnel.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Does the organization maintain an organized and equipped crisis response force?	Identify crisis response force. Review documentation describing crisis response force.
	Does the crisis response force receive adequate training?	Review documentation describing crisis response force.
	How many personnel are available within the facility?	Review documentation describing crisis response force.
	Outside the facility, how many additional security forces could be brought with: <ul style="list-style-type: none">■ One hour notice■ Four hour notice	Review documentation describing crisis response force.
	Has liaison been established with local, state, and federal law enforcement agencies whereby early warning of a threat situation will be provided?	Review documentation describing crisis response force. Review correspondence with local, state, and federal law enforcement agencies.
	Does security force personnel record or report their presence at key points in the facility by means of: <ul style="list-style-type: none">■ Portable watch clock■ General watch clock stations■ Telephones?■ Two way radio communications equipment■ Other Are guard assignments, times and patrol routes varied at frequent intervals avoiding establishing routine? If yes, what are the intervals	Review documentation that indicates reporting mechanism used by security force personnel to identify their presence at key points in the facility.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.18 Personnel and Vehicle Movement Control	Is a pass or badge identification system in effect to identify all personnel within the confines of restricted areas?	Review procedures for controlling the movement of personnel and vehicles.
	Are personnel who require infrequent access to a restricted area or have not been issued a permanent pass or badge for such, treated as visitors, and issued a visitors badge or pass?	Review procedures for controlling the movement of personnel and vehicles.
	Do guards at contract points compare badges to bearers, both upon entry and exit? If no upon entry only? If no, Upon exit only?	Review procedures for controlling the movement of personnel and vehicles.
	Is the personnel identification and control system supervised at all levels?	Review procedures for controlling the movement of personnel and vehicles.
	Are badges and serial numbers recorded and controlled by rigid accountability procedures?	Review procedures for controlling the movement of personnel and vehicles.
	Are lost badges replaced with badges bearing different serial numbers?	Review procedures for controlling the movement of personnel and vehicles.
	Have procedures been established that provide for issuance of temporary badges for individuals who have forgotten their permanent badges?	Review procedures for controlling the movement of personnel and vehicles.
	Are badges of such design and appearance as to enable guards, and other personnel, to recognize quickly and positively the authorizations and limitations applicable to the bearer	Review procedures for controlling the movement of personnel and vehicles.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are procedures in existence to ensure the return of identification badges upon termination of employment of assignment?	Review procedures for controlling the movement of personnel and vehicles.
	Have effective visitor escort procedures been established when necessary?	Review procedures for controlling the movement of personnel and vehicles.
	Are visitors escorted within restricted areas when necessary?	Review procedures for controlling the movement of personnel and vehicles.
	Are permanent records of visits maintained? If yes, by whom are these records kept?	Review procedures for controlling the movement of personnel and vehicles.
	Are POVs and contractor vehicles, which are allowed routine access to the installation, registered with the security office?	Review procedures for controlling the movement of personnel and vehicles.
	Are random administrative inspections made of automobiles?	Review procedures for controlling the movement of personnel and vehicles.
3.19 Security Equipment	<p>Does the Security force have sufficient vehicles to maintain patrols, respond to alarms and emergencies and maintain supervision?</p> <p>Are security force vehicles equipped with:</p> <ul style="list-style-type: none">■ Signs conspicuously identifying the vehicles as security police vehicles?■ Emergency exterior overhead lights?■ Electronic siren? <p>Do security force vehicles have relatively low mileage?</p>	Review documentation indicating security equipment inventory.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	How often do the security officers and supervisory personnel review the firearms and ammunition requirements to ensure their accuracy?	Review documentation indicating review of the firearms and ammunition requirements.
	Do observation towers provide security personnel with observations of security areas?	Review location and visibility of observation towers.
	What type of ammunition is used by armed security force personnel?	Review documentation indicating the type of ammunition used by armed security force personnel.
	Is ammunition properly secured for and issued only to authorized personnel?	Review documentation indicating procedures for the storage and distribution of ammunition.
	Are weapons stored and secured when not in use?	Review documentation indicating procedures for the storage and distribution of weapons.
	Are duties other than those related to security performed by security personnel?	Review job descriptions of security personnel. Review contractual documentation from security contractor, if applicable. Interview security personnel.
	Does the organization provide device and specialized equipment for use by the security force?	Review documentation indicating devices and/or specialized equipment distributed to the security force.
	Does the organization provide security force personnel with individual equipment?	Review documentation indicating devices and/or specialized equipment distributed to the security force.
3.20 Security Measures	Does the organization have a loss prevention plan?	Document and review security measures.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	What is the date of the organizations most recent risk and threat analysis?	Review documentation detailing risk and threat analysis.
	Have areas been designated by the organization as restricted areas as necessary?	Review documentation indicating location and perimeters of restricted areas.
	Are the basic security measures for restricted areas in effect?	Review documentation defining the basic security measures for restricted areas. Compare definitions to current state.
	Are all restricted area points appropriately posted?	Visit restricted area points.
	Are security measures in effect to protect: <ul style="list-style-type: none">■ Electrical power supplies and transmission facilities■ Communications centers/equipment■ Arms ammunition and dangerous cargoes?	Review security measures in effect.
	Are physical surveys of the facilities conducted at least annually under the auspices of the security office?	Review documentation indicating that physical surveys are conducted.
	What is the date of the most recent physical security inspection, audit, or review by an immediate supervisor in the facility?	Review documentation detailing recent physical surveys. Identify person who conducted survey. Interview surveyors.
	Does the facility have an after hours or weekend restricted area security check by the security force?	Review documentation indicating the existence of an after hours or weekend restricted area security check by security force.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are the results of security checks promptly reported to the facility security officer?	Identify reporting process for security checks to the facility security officer.
	Does the facility have a privately owned vehicle (POV) parking plan? If yes, does it include: <ul style="list-style-type: none">■ Restriction of POV parking in exclusive and limited areas?■ Fence/enclave parking in controlled areas?	Review parking plan for POV.
	Does the facility have a traffic control program?	Review documentation indicating the existence of a traffic control program.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.21 Barriers and Openings	<p>Does the fenced portion of the facility meet the minimum specification for security fences?</p> <p>Is it of chain link (cyclone) composition?</p> <p>Is it constructed of 9 gauge or heavier wire?</p> <p>Is the mesh opening no larger than two inches?</p> <p>Is the salvage twisted and barbed at top and bottom?</p> <p>Is the bottom of the fence within two inches of solid ground?</p> <p>In areas where the fence exceeds two inches from solid ground, have compensatory measures been taken?</p> <p>Is the top guard strung with barbed wire (or barbed tape/razor edge) and angled outward from the protected site and upward at a 45-degree angle?</p> <p>Is the fence at least eight feet in height including outrigger in all required areas?</p>	<p>Review security of barriers and openings to the facility.</p>
	<p>Does the facility provide for security force inspection of the security barrier including clear zone at least once per month?</p> <p>Are deficiencies noted?</p> <p>Are remedial actions promptly effected?</p>	<p>Review documentation indicating procedures for security force inspection of the security barrier.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is masonry wall used as part of facility barriers? If yes, do they provide security equivalent to that provided by the security barrier?	Review architectural documents for facility barriers.
	Are all openings properly secured?	Review architectural documents for facility barriers.
	Does a building form a part of the barrier? If yes, are additional security measures provided?	Review architectural documents for facility barriers.
	Are openings such as culverts, tunnels, and manholes for sewers and utility access and sidewalks, which permit access to the facility restricted and secured?	Review architectural documents for facility barriers.
	Are all portals in perimeter barriers guarded and or secured?	Review architectural documents for facility barriers.
	Do the gates and/or other entrances in perimeter barriers exceed the number required for safe and efficient operations?	Review architectural documents for facility barriers.
	Are all perimeter barrier portals equipped with secure locking devices? Are they locked when not in used?	Review architectural documents for facility barriers.
	Do all gates provide protection equivalent to that provided by the barrier of which they are part?	Review architectural documents for facility barriers.
	Are prescribed clear zones maintained on both sides of the restricted area barriers?	Review architectural documents for facility barriers.
	If clear zone requirements cannot be met, have compensatory security measures been implemented?	Review architectural documents for facility barriers.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are any perimeters protected by intrusion detection systems (IDS)?	Review architectural documents for facility barriers. Review electronic security system documents.
3.22 Protective Lighting	<p>Is the perimeter and restricted areas provided protective lighting?</p> <p>If Yes:</p> <ul style="list-style-type: none">■ Does the protective lighting meet adequate intensity requirement?■ Are the zones of illumination from lamps directed downward and away from guard personnel?■ Is perimeter protective lighting utilized so that security force personnel remain in comparative darkness?■ Are lights checked at least weekly for proper operation prior to darkness?	Review lighting specifications in architectural documents.
	Are repairs to lights and replacement of inoperative lamps effected immediately or in a reasonable time?	Review documentation indicating procedures for light replacement.
	Is additional lighting provided at active portals and points of possible intrusion?	Review lighting specifications in architectural documents.
	Does the facility have a dependable source of power for its protective lighting system?	Review lighting specifications in architectural documents.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Does the facility have a dependable auxiliary (emergency) source of power for protective lighting? If yes, is the power source protected?	Review lighting specifications in architectural documents.
	Are there provisions for standby or emergency protective lighting? If yes, is the standby or emergency equipment tested at least monthly?	Review lighting specifications in architectural documents.
	Can the emergency backup power supply be rapidly switched into operation when needed?	Review lighting specifications in architectural documents.
	Is the emergency backup power supply self started?	Review lighting specifications in architectural documents.
	Is the protective lighting/emergency or standby power source located within the restricted area?	Review lighting specifications in architectural documents.
	Is parallel circuitry used in the wiring?	Review lighting specifications in architectural documents.
	Are multiple circuits used? If yes, are proper switching arrangements provided?	Review lighting specifications in architectural documents.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	<p>Are switches and controls:</p> <ul style="list-style-type: none">■ properly located, controlled and protected?■ weather proof and temper resistant?■ readily accessible to security personnel?■ located so that they are inaccessible from outside the perimeter barrier? <p>Is there a centrally located switch to control protective lighting?</p>	<p>Review lighting specifications in architectural documents.</p>
	<p>Is the protective lighting system designed and locations recorded so that repairs can be made rapidly in an emergency?</p>	<p>Review lighting specifications in architectural documents.</p>
	<p>Are materials and equipment in shipping and storage areas properly arranged to provide adequate lighting?</p>	<p>Review lighting specifications in architectural documents.</p>
	<p>If bodies of water form a part of the perimeter, is adequate lighting provided where deemed appropriate?</p>	<p>Review lighting specifications in architectural documents.</p>
3.23 Intrusion Detection System	<p>Does the facility employ IDS?</p>	<p>Examine intrusion detection systems.</p>
	<p>Are IDS signals monitored at one central point? Is the security force response initiated from that point?</p>	<p>Review documentation describing use of IDS.</p>
	<p>Are all sensor equipment, doors, drawers and removable panels secured with key locks or screws and equipped with tamper switches?</p>	<p>Review documentation describing use of IDS.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Have power supplies been protected against overload by fuses or circuit breakers?	Review documentation describing use of IDS.
	Are annunciator, control, and display subsystems located in a separate areas/closed off from public view?	Review documentation describing use of IDS.
	Is the system backup by security alert teams?	Review documentation describing use of IDS.
	Is the alarm system for active areas or structures placed in access mode during normal working hours?	Review documentation describing use of IDS.
	Is the system tested prior to activation?	Review documentation describing use of IDS.
	Is the system inspected at least monthly?	Review documentation describing use of IDS.
	Is the exterior IDS waterproof?	Review documentation describing use of IDS.
	Is there an alternate or independent power source available for use on the system in the event of power failure?	Review documentation describing use of IDS.
	Is the emergency power source designed to cut in and operate automatically when AC power goes down?	Review documentation describing use of IDS.
	Do trained and properly cleared personnel maintain the IDS system?	Review documentation describing use of IDS.
	Are frequent tests conducted to determine the adequacy and promptness of response to alarm systems?	Review documentation describing use of IDS.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.24 Employee Security Education Program	Does the activity have a current employee security education program addressing facility security management?	Review documentation describing employee security education program.
	Are all assigned personnel provided facility security indoctrination?	Review documentation describing employee security education program.
	Is formal security education training conducted at least annually for all personnel?	Review documentation describing employee security education program.
	Are all personnel indoctrinated in security procedures, which apply in the performance of their duties?	Review documentation describing employee security education program.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	<p>Is yes, does the program cover such topics as:</p> <ul style="list-style-type: none">■ Pass and badge systems■ Privately owned vehicle identification and control■ Random package and vehicle inspection?■ Procedures for prompt reporting of security breaches?■ Layout of the facility to which the security force is assigned?■ Means/avenues by which the facility may be accessed?■ Types of operations on the facility that should be expected?■ General security topics? <p>Are local law enforcement agencies asked to actively participate in pertinent portions of this program?</p>	Review documentation describing employee security education program.
3.25 Security Force Training	Does the facility provide security force training?	Examine documentation describing security force training.
	Does the facility provide lesson plans to cover all facets of security and law enforcement?	Examine documentation describing security force training.
	Is outside law enforcement/security training provided?	Examine documentation describing security force training.
	If yes- list schools:	



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are individual training records maintained for security force personnel?	Review documentation indicating the existence of training records for security force personnel.
	Do all security force personnel who are required to bear firearms, receive training?	Examine documentation describing security force training.
	Do all security personnel receive indoctrination in the use of force?	Examine documentation describing security force training.
3.26 Security Force Communications	Does the activity security force have its own communications system with direct communications between security headquarters and security elements?	Review documentation describing security force communications.
	Is there an auxiliary power supply for the communications systems?	Review documentation describing auxiliary power supply.
	Is there sufficient equipment to maintain continuous communications with each element of the security force?	Review documentation describing security force communications.
	Is there alternate means of communication available to the security force?	Review documentation describing security force communications.
	Is yes, is it comparable to the main source of communications?	Review documentation describing security force communications.
	What is the primary means of communication for the security force?	Review documentation describing security force communications.
	What is the alternative means of communications for the security force?	Review documentation describing security force communications.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Radio communications: Are proper radio procedures practiced? Is all communications equipment properly maintained? Are there at least two dedicated radio frequencies for security force use? Are portable radios equipped with multiple frequency capability? Are portable radios equipped with an automatic tilt or switch activated duress frequency?	Review documentation describing security force communications.
	Does the security force use a duress code for emergency situations?	Review documented procedures for emergency situations.
	Is the duress code changed at least monthly?	Review documented procedures for emergency situations.
	Is the communications center afforded adequate physical security against armed intrusion?	Review documented procedures for emergency situations.
	Are communications systems capable of being used to transmit instructions to all key posts simultaneously in a rapid and timely manner?	Review documentation indicating capabilities of communication system.
3.27 Sabotage	Do procedures exist to protect your organization against industrial sabotage?	Review documentation indicating sabotage protection procedures.
	Do procedures exist to protect your organization against radiological sabotage?	Review documentation indicating radiological sabotage protection procedures.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Have measures been taken to protect the health and safety of the public?	Review documentation indicating the procedures to protect the health and safety of the public.
3.28 Protection of Targets	A target is a physical item or information that an adversary wishes to acquire, destroy, or modify. Has your organization identified targets within the facility (vaults, labs, shipment trucks, equipment room, etc.)?	Review documentation identifying targets. Examine procedures for protecting targets.
	If so, have special measures been taken to secure these targets?	Examine procedures for protecting targets.
	Has “One of-a-kind” equipment been considered and protected sufficiently?	Review documentation identifying targets.
	Have you determined the consequence of target of loss, including type and quantity of material or weapon, effect on health and safety of public, effect on national security?	Review documentation indicating the appropriate response to the loss of a target.
3.29 Threat Estimation	Has your organization obtained local threat data by defining the site-specific threat to the facility?	Retrieve and examine threat data.
	To assist with the definition of local threats have you contacted your local FBI office, State Police, Sheriff’s office and local police department, nearby military special investigations or criminal investigations unit, Alcohol, Tobacco, and Firearms (ATF), Treasury, drug Enforcement Agency (DEA), or other local offices of federal law enforcement agencies?	



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.30 Information Gathering	Are facility tours conducted?	Explore avenues of information gathering.
	Are architectural diagrams and alarm system prints available?	Review the availability of documentation.
	Are interviews conducted with facility personnel (management and workers)? It is important to interview those who know how safeguards actually work, not just how they <u>should</u> work.	Review documentation of interviews conducted with facility personnel.
	Are safeguards, security, and material control and accountability plans available?	Review availability of safeguards, security and material control and accountability plans.
	Has a diagram of your facility been drawn?	Review availability of a facility diagram.
	If yes, does the diagram focus on issues relevant to safeguards and security?	Review facility diagram.
	Does the diagram highlight representative features? It should not indicate every emergency exit, for example, if all are essentially the same.	Review facility diagram.
	Does the diagram indicate the location of targets?	Review facility diagram.
	Does the diagram highlight physical areas and protection layers (the set of path elements separating two areas)?	Review facility diagram.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Have common path elements (a physical route or passageway from one area to another) been considered? These include: gates, portals, and emergency exits; fences, isolation zones, and overpasses; surfaces, roofs, floors, and windows; ducts, tunnels, and effluent-removal systems; helicopter flight paths.	Review facility diagram.
3.31 Intrusion Detection	Have primary sensors that detect unauthorized passage or penetration been installed on the interior of the facility?	Review intrusion detection capabilities of the facility.
	Have primary sensors that detect unauthorized passage or penetration been installed on the exterior of the facility?	Review intrusion detection capabilities of the facility.
	Have alarm assessment mechanisms been installed?	Review intrusion detection capabilities of the facility.
	Do alarm systems detect contraband?	Review intrusion detection capabilities of the facility.
3.32 Defeating Delay	Have delays that are inactive during certain states been considered, such as vault doors and gates?	Examine existing delays both inactive and active that may affect threat elimination response time.
	Have activated delays such as smoke generators and vault doors been taken into account?	Examine existing delays both inactive and active that may affect threat elimination response time.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
3.33 Insider Threats	Have insider types and acts been considered? Insider threats include anyone with access to the facility (or inside knowledge of the operations). Insider criminals are among the most difficult and dangerous adversaries to defend against.	Identify and review insider threats.
	Are assessments performed that view the facility from an adversary's perspective?	Review documentation indicating that assessments are performed from an adversary's perspective.
	For each person that has access to the facility, do you have information that reflects: access to critical facility areas, keys or combinations held or easily acquired special authority or job privilege, special skills or knowledge?	Review information available regarding personnel access to facility.
	To protect your facility against insiders, have inventories been consolidated and reduced?	Review inventory consolidation and reduction procedures.
3.34 Outsider Threats	Have outsider types and acts been considered such as terrorists, criminals, psychotics and anti-nuclear extremists?	Identify and review outsider threats.
	Have outsider attacks been documented?	Review documentation indicating outsider attacks.
	Have intelligence-gathering agencies been utilized for gathering data about outsider threats?	Review documentation indicating that intelligence-gathering agencies have been contacted.
	Have detection, delay and response options been explored?	Review documentation indicating that detection, delay and response options have been explored.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Has the physical location of detectors been explored?	Review documentation indicating the physical location of detectors.
	Has protection during uncommon facility states been considered?	Review documentation describing protection of facility during different states.
3.35 Upgrade Analysis	Are iterative safeguard evaluations conducted to identify upgrades and achieve effective protection? Generally, upgrades imply physical change in the protection system. However, organizational changes, administrative and procedural and re-deployment of existing resources constitute upgrades if they reduce the risk.	Review documentation indicating that safeguard evaluations are conducted to identify upgrades and achieve effective protection.
3.36 Key Control	Describe key control system.	Review documentation describing key control systems.
	Who is responsible for key control?	Review documentation describing key control systems.
	How many master keys, which provide access to all locks, are there?	Review documentation describing key control systems.
	Who has been issued master keys? What are their names, positions and what is the key number?	Review documentation describing key control systems.
	Are keys signed for?	Review documentation describing key control systems.
	Are all keys accounted for?	Review documentation describing key control systems.
	Is issuance of keys recorded?	Review documentation describing key control systems.
	If yes, is report kept up to date?	Review documentation describing key control systems.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are keys removed from vehicles at night and on weekends?	Review documentation describing key control systems.
	Describe the procedure for return of keys when an employee is terminated or transferred.	Review documentation describing key control systems.
3.37 Trash Disposal	Who provides the facility's trash disposal?	Review trash disposal process.
	How often is trash removed?	Review trash disposal process.
	Is trash periodically inspected?	Review trash disposal process.
	Is trash removed from facility under supervision?	Review trash disposal process.
3.38 Lobby	How many hours per day is the lobby open?	Review lobby access policy.
	What time does the lobby open/close?	Review lobby access policy.
	Is any control exercised over personnel movement during this time?	Review lobby access policy.
	Is it possible to have any personnel control in the lobby during open periods?	Review lobby access policy.
	Describe controls currently in force.	Review lobby access policy.
	How many banks of elevators are there in the lobby?	Review lobby access policy.
3.39 Custodial Personnel	Is the custodial work in the building done by building employees or by contract personnel?	Review documentation indicating custodial access controls.
	How are custodial passkeys distributed?	Review documentation indicating custodial access controls.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	During what hours do custodial personnel work?	Review documentation indicating custodial access controls.
	How is custodial service supervised?	Review documentation indicating custodial access controls.
	Are these emergency exits tested on a monthly basis to ensure that the alarms are working properly?	Determine area responsible for testing exits. Obtain evidence of testing for last 2 quarters.
	Are emergency exits equipped with an automatic closing device?	Test to ensure that each emergency exit in the area is equipped with such a device.
Data Centers		
4. Controls are in place to ensure that the identification and access rights of users as well as the identity of system and data ownership are established and managed in a unique and central manner to obtain consistency and efficiency of global access control.	Is all computer and telecommunications equipment in a physically secured data center?	Verify that no computer and telecommunications equipment exist outside a secured data center.
	Has the data center been assessed for risk?	Assess the data center for risk.
	Is access to telephone/riser closets adequately controlled?	Determine whether closets are locked and how keys are secured. Evaluate whether only appropriate, authorized individuals possess keys.
	Are telephone/riser closets clean and free of miscellaneous equipment?	Perform walk-through of each closet and determine whether closets are neat and clean.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	If a room contains equipment that will be supported by MORE THAN ONE ORGANIZATIONAL ENTITY (i.e. department, vendor, etc.), is a recorded CCTV camera used to monitor the person entering the room? One exception to this requirement is to have the approved vendor escorted by a department employee for the full amount of time the vendor is in the room. Also, it is important to ensure that he/she does not have access via the card key entry system, so that he/she cannot enter alone.	Verify that if a room contains equipment that will be supported by multiple entities (departments, vendors, etc.) a recorded CCTV camera is used to monitor the person entering the room. Verify that the tapes are retained for a minimum of seven days.
Physical Access Lists and Visitor Logs to Data Centers		
5. Controls are in place to ensure that adequate control measures are imposed to safeguard equipment and facilities	Is there an access list posted at the data center entrance?	Obtain current list of employees and verify that access list is up to date. You may need to obtain a list from HR listing all employees who have transferred or left the area to verify whether the list is current.
	Is there a process to review the access list on a quarterly basis to ensure it is current?	Obtain procedures as well as evidence that review was conducted for the last 2 quarters.
	Do only authorized individuals (including authorized employees, consultants, or vendors) have access to the tech/Comm room or data center and do the names of those authorized match the access list posted on the door?	Obtain a listing from the Card Key System and reconcile against an HR listing of employees who have left the area and current vendor/consultant lists who support equipment in the facility.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Do documented procedures exist for the admittance and control over visitors to the tech/communications room or data center? NOTE: If an outsourcing agreement exists, then vendor personnel who require access to perform their job are not considered visitors.	Verify the existence of these procedures.
	Do authorized department personnel while working within the secured Tech/Comm Room or data center escort all visitors?	Verify that procedures document this requirement and observe process when visitors are present.
	Does a visitors log exist for all non-authorized personnel to sign-in upon entering the Tech/Comm Room or data center?	Select 5 completed pages from the logbook for review. Verify that the log contains the proper verification items.
	Does it require: date of visit, individual's name, purpose of visit, time-in and time-out and initials of employee authorizing the visit?	Verify that date of visit, individual's name, purpose of visit, time-in and time-out and initials of employee authorizing the visit are present on the samples.
	Is management required to review the visitor logs weekly to ensure that logs are complete and do they evidence their review by signing the log in the appropriate space?	Select a 5-page sample from the logbook and verify entries are complete and that there is evidence of management review.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
Physical keys, Card keys and Cipher locks		
6. Controls are in place to ensure that adequate physical security measures are imposed to safeguard equipment and facilities	Is a recorded Card key system used to enter and exit all legacy and new Installations as specified by Corporate Security?	Verify that a Recorded Card key system is used to enter and exit all legacy and new Installations as specified by Corporate Security, by observation.
	Is there a process to periodically inventory the card keys to ensure that none have been lost or stolen?	Obtain evidence of most recent card inventory. Spot check items on the list to ensure inventory is complete.
	Is there a process for management to periodically (i.e., at least semi-annually) review card key access listings to ensure that only authorized individuals have access to the facility?	Obtain the results from the last review. Ensure all affected areas of management have had an opportunity to review the listing.
	Is there a policy that requires management to obtain card keys from terminated or transferred employees?	Obtain procedures and list of employees who have left the area from HR. Verify that cards for employees who have left have either been assigned to other users or are deactivated.
	Are unused card keys kept in a secured location and kept in a deactivated state?	Meet with security personnel to determine where cards are secured. Review card list or card key system itself to determine whether cards are deactivated. Record observation.
	Does the facility have a fail-safe design or manual override capability if the Card Key Access System fails?	Verify the existence of the fail-safe through observation or documentation from the manufacturer.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	If a cipher lock is used, compensating controls must be used. Is there a process for management to periodically (i.e., at least semi-annually) review cipher lock access listings to ensure that only authorized individuals have access to the facility?	Obtain the results from the last review. Ensure all affected areas of management have had an opportunity to review the listing.
	Does a procedure exist to change the cipher lock at least quarterly or when an employee leaves the area?	Verify the existence of the procedure stating these controls.
	Is the key to change the cipher lock combination kept in a secured location (i.e., Tel-key box or safe)?	If key is in the Tel-key box, answer Facilities - Tel-Key Box Section.
	Is a logbook of cipher lock changes kept?	Verify that changes were made quarterly or when an employee left, by reconciling with a HR listing of employees who have left the area. Verify that all log entries are complete.
	Does the facility have a fail-safe design or manual override capability if the cipher lock system fails?	Verify the existence of a fail safe or manual override through observation or documentation from the manufacturer.
	Is access to the Tech/Comm Room or data center controlled through the use of physical keys?	
	Is there a list of individuals who have keys to the facility and is it appropriate for all those on the list to have these keys?	Verify with management that the appropriate individuals have keys.
	Is a Tel-key box used by the facility to secure keys and/or passwords to sensitive ID's?	If you determine through the course of your review that a Tel-key box is needed, then record this as an issue as well.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is the Tel-key box under dual control?	Observe the process to open the box. Obtain a list of individuals who possess these keys and their location. Make sure that one individual cannot dominate the entry process.
	Is there an inventory of items inside the Tel-key box?	Obtain inventory and sample items in Tel-key box to ensure that the inventory is current
	Is there a logbook to record what is removed and returned to the Tel-key box? Does the logbook contain Date, Time, Reason for removal including Trouble ticket #, and the initials of both individuals who opened the Tel-key box to remove the item?	Remove 3 completed pages from the log. Verify completeness of columns & entries. Select 6 entries from sampled pages & trace to trouble ticket # or other authorizing paperwork.
	Does management review the Tel-key log monthly to ensure that entries are complete and is there evidence of such a management review?	From 3-page sample, ensure that a management review was performed monthly.
	Is the Tel-key box process documented in a procedure manual?	Verify that the Tel-Key Box procedures are documented in the procedure manual.
	<p>If tech/comm room is shared among multiple business units and/or vendors, is equipment kept in locked cabinet?</p> <p>Are keys to these cabinets secured?</p>	Spot check several cabinets and verify that cabinets are locked. Determine controls over cabinet keys.
Passwords		



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
7. Passwords, tokens, or other devices are used to identify and authenticate users.	<p>Are passwords</p> <ul style="list-style-type: none">■ unique for specific individuals, not groups;■ controlled by the assigned user and not subject to disclosure;■ changed periodically—every 30 to 90 days;■ not displayed when entered;■ at least 6 alphanumeric characters in length;■ prohibited from being shared, and■ prohibited from reuse for at least 6 generations?	<p>Review pertinent policies and procedures.</p> <p>Interview users.</p> <p>Review security software password parameters.</p> <p>Observe users keying in passwords.</p> <p>Attempt to log on without a valid password; make repeated attempts to guess passwords.</p> <p>Assess procedures for generating and communicating passwords to users.</p>
	<p>Is the use of names or words is prohibited?</p>	<p>Review a system-generated list of current passwords.</p> <p>Search password file using audit software.</p>
	<p>Are vendor-supplied passwords replaced immediately?</p>	<p>Attempt to log on using common vendor supplied passwords.</p> <p>Search password file using audit software.</p>
	<p>Are generic user IDs and passwords used?</p>	<p>Interview users and security managers.</p> <p>Review a list of IDs and passwords.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are password protected screen savers used on all desktop computers?	Verify password protected screen savers are installed and locking out within a specified time period on all desktop computers by sampling them for compliance.
	Are attempts to log on with invalid passwords limited to about three attempts?	Repeatedly attempt to log on using invalid passwords. Review security logs.
	Are personnel files automatically matched with actual system users to remove terminated or transferred employees from the system?	Review pertinent policies and procedures. Review documentation of such comparisons. Interview security managers. Make comparison using audit software.
	Are password files encrypted?	View dump of password files (e.g., hexadecimal printout).
	For other devices, such as tokens or key cards, do users: <ul style="list-style-type: none">■ maintain possession of their individual tokens, cards, etc, and■ understand that they must not loan or share these with others, and must report lost items immediately?	Interview users: To evaluate biometrics or other technically sophisticated authentication techniques, the auditor should obtain the assistance of a specialist.
Network Management Systems (NMS)		
8. Network Management Systems (NMS)	Are all terminal access methods (i.e., dial-in, LAN, hard-wired) for the NMS listed?	Obtain dial-in access list for all NMS in use. Compare list against each NMS configuration.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is there a description of each NMS and are the networks they support documented in the procedures?	Each NMS in use must have written procedure for designated network. Operational procedure should be in PCM manual.
	Are all network control and monitoring systems in a physically controlled area?	Ensure that physical security to Network control and monitoring systems approved by manager. Check access list to controlled area against organization chart.
	If dial-in access is allowed to the NMS, are dial-in access controls in place (e.g., manual log or callback security)?	If the remote dial-in access to NMS is allowed. Operations personnel must have: <ul style="list-style-type: none">■ Ready access to the list of network User ID's, location, and telephone contact number.■ The facility to rapidly disable any individual network User ID. Maintain current log for all dial-in access activity. Systems must have unlisted phone numbers.
	Are security administration procedures (i.e., ID creation, review of security administration activity, violation monitoring, emergency access, and periodic review of entitlements) in place for each network management system?	Review procedures



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is a segregation of duties maintained between the individuals performing the security administration function for each NMS and the individuals performing the network management and monitoring functions?	Look at ACLs to determine if security and system administration function is segregated.
	Are the NMS privileges of individuals in the area under review appropriate for their job function?	Review organization chart with roles and responsibilities.
	Are NMS IDs shared by more than one operator or technician?	Look at user ID file to determine if generic IDs exist.
	If shared IDs are used, is it because legacy systems are used where separate IDs are not technologically feasible? Or, are the IDs, which are shared used solely for monitoring purposes, and have read or inquiry access only?	See above
Security Software		
9. Logical Controls over Data Files and Software Programs	Is security software used to restrict access?	Interview security administrators and system users.
	Is access to security software restricted to security administrators only?	Review security software parameters.
	Are computer terminals automatically logged off after a period of inactivity?	Observe terminals in use. Review security software parameters.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are inactive user accounts monitored and removed when not needed?	Review security software parameters. Review a system generated list of inactive logon IDs, and determine why access for these users has not been terminated.
	Do security administration personnel set parameters of security software to provide access as authorized and restrict access that has not been authorized including access to data files, load libraries, batch operational procedures, source code libraries, security files, and operating system files?	Determine library names for sensitive or critical files and libraries, and obtain security reports of related access rules. Using these reports, determine who has access to critical files and libraries and whether the access matches the level and type of access authorized.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
DBMS		
10.1 Logical controls over a database	<p>Have database management systems (DBMS) and data dictionary (DD) controls been implemented that:</p> <ul style="list-style-type: none">■ restrict access to data files at the logical data view, field, or field-value level;■ control access to the DD using security profiles and passwords;■ maintain audit trails that allow monitoring of changes to the DD;■ provide inquiry and update capabilities from application program functions, interfacing DBMS or DD facilities?	<p>Review pertinent policies and procedures.</p> <p>Interview database administrator.</p> <p>Review DBMS and DD security parameters.</p> <p>Test controls by attempting access to restricted files.</p>
	Is the use of DBMS utilities limited?	Review security system parameters.
	Are access and changes to DBMS software controlled?	Review procedures and change control documentation.
	Is the access to security profiles in the DD and security tables in the DBMS limited?	Review procedures for access.
10.2 Network Management Systems (NMS)	Are network topology diagrams current for each network that supports the production environment?	Review each network topology and verify accuracy of the information against the actual network configuration. Use management system data for verification and cross-referencing.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are detailed network circuit diagrams current?	Sample 10% of network circuits. Choose several linkages from the topology diagrams and trace diagrams to the physical equipment, Check for Demark ID's, modems, cable switching equipment, label ID's, cabinet ID's, servers, router, etc.
Remote Access		
11.1 Logical controls over telecommunications access	Are dial-in phone numbers published and are they periodically changed?	Review pertinent policies and procedures. Review documentation showing changes to dial-in numbers. Review entity's telephone directory to verify that the numbers are not listed.
11.2 Dial Backup (DBU)	Are all Dial Backup lines that are defined to the network listed?	Obtain a list of DBU lines for use by interviewing management.
	Do procedures exist for authorizing, invoking, monitoring and testing dial backup for certain portions of the network?	Obtain procedures and ensure that procedures address all concerns.
11.3 Remote Access	If session level encryption is used (e.g., IRE) and activation is dependent on some type of physical connection, are users prohibited from gaining access via alternate means (i.e., different phone numbers)?	Obtain reports from management system to identify user listing, devices, application names and unauthorized access activity. Check if trouble tickets are opened for illegal connections.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is dial-in access to all production resources restricted to authorized personnel via either challenge response, dynamic password exchange, and approved cryptographic techniques, or emergency procedures, which incorporate compensating controls?	All personnel, consultants, and vendor dial-in access should use dynamic password tokens (i.e. SecureID, DESGOLD, etc.) cards for user authentication. Obtain users dial-in list and verify approved authentication use.
	Are all Internet gateways to and leased lines interfacing with external networks are protected by a firewall?	Verify that backbone networks and business supported LAN's and WANs protected by firewalls. Firewalls must be configured to provide; user identification, destination screening, and service restrictions (i.e. Telnet, FTP)
	Does an inventory exist of the dial-in devices, which includes their location?	Access to the network, User ID, location and telephone contact number must be documented.
	Does a formal process exist to request dial-in access, which requires supervisor or business relationship approval?	Procedure must be in place regardless of whether the dial access facilities are owned and operated by the internal organization, or by external service provider. Verify procedures for approved dial-in access.
	If private or public dial-in access is being used, how is this access tracked and controlled?	Obtain reports to validate dial-in access. Reference to Information Security Admin reports to identify failed attempt and unauthorized access. Obtain violation-logging records for verification.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
Encryption and Related Applications		
12.1 Cryptographic tools	Have cryptographic tools been implemented to protect the integrity and confidentiality of sensitive and critical data and software programs?	To evaluate cryptographic tools, the auditor should obtain the assistance of a specialist.
12.2 Transaction Authorization	Do policies exist to ensure that where appropriate, controls are implemented to provide authenticity of transactions? This requires use of cryptographic techniques for signing and verifying transactions.	Review policies to determine if they exist for authenticity of transactions.
12.3 Cryptographic Key Management	Are the physical and logical encryption keys secured under dual control?	Review dual control procedures of logical and physical encryption keys. Some encryption devices have physical keys; others have a module that plugs into the unit to change the logical keys. Key A and B must be separated and maintained by two different party or people. This procedure applies to internal or external controls.
	Are encryption devices properly locked and are physical keys removed from the units?	Select cabinets with encryption devices installed. Each Tag must have, encryption unit #, CKT ID. Unused keys must be Tagged. Verify if encryption devices locks are in locked position and physical keys in Telkey box.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	If encryption keys are automatically changed, are alarms/events in place to notify management when devices are inoperable or set to the bypass mode?	Review encryption devices management system alarms events for unsuccessful DAILY key exchange or BYPASS conditions. Devices that are not connected to management system the above events can be obtained directly from unit. Look into encryption management option. Evidence must be signed and dated by manager. Note: each unit can store up to 99 events, then buffer is over written with new data.
	Is the organization notified within a designated number of hours whenever a particular device is placed in bypass mode?	Reference to SLA for user notification process. Memo or trouble ticket should be used for notification if required. Verify if user has requested this type of service.
	Are alarms reviewed in real time? Are procedures in place for performing this review?	Institute procedure to review alarms in real time and develop review process. Manager signature and date must exist. If checkoff list is utilized, verify if all major alarms are displayed in real time and corrective action taken for each event.
	Does the cryptographic key distribution methodology in place comply with the ANSI X9.17 and X 9.24 Standards?	DES is approved standard.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is master key encryption keys change procedure documented and in place?	Management must sign logs. Review procedure for MASTER key encryption generation, distribution scheme and records keeping. Reference to vendor manuals for detail process. For manual device key must be changed at least once a year. Devices that utilize management system key can be distributed automatically.
	Do the encryption devices that have manual key exchanging features use tamper proof encryption key transportation and storage device?	Logs must be dated and signed by management. Cryptographic hardware must be tamper proof as specified in Federal Information processing Standards (FIPS) 140-1. Information must be protected from unauthorized access and have automatic erasure.
	Are all data that requires protection encrypted for all systems that process sensitive information?	Standards require encryption over all links that transmit this type of data through which any bank transaction is transmitted. Identify supported business with sensitive information to ensure if Restricted and Confidential data is secured. Reference to risk level analysis or SLA documentation if available.
	Do you maintain a list of encrypted and unencrypted circuits and which businesses each circuit supports?	Reference to SLA for encryption requirement and data owner responsibility. Obtain encrypted and unencrypted circuits inventory list. Identify which businesses are not compliant. Verify encrypted circuits supported businesses.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are ALL network data transmissions that leave government property (including cases where government personnel do not occupy contiguous floors of a building) encrypted?	Identify data circuits that transmit through non-government owned property or floors. Contact businesses and obtain approval of exposure.
	Are all default encryption keys changed that are provided by the vendor? Are these keys changed after each new software release?	Examine encryption devices configuration against standards.
12.4 Non-Repudiation	Do policies exist for ensuring that, where appropriate, transactions cannot be denied by either party, and controls are implemented to provide non-repudiation of origin or receipt, proof of submission, and receipt of transactions? This can be implemented through digital signatures, time stamping and trusted third parties.	Review policies relating to digital signatures.
Monitoring		
13.1 Audit trails are maintained	Is all activity involving access to and modifications of sensitive or critical files logged?	Review security software settings to identify types of activity logged.
13.2 Actual or attempted unauthorized, unusual, or sensitive access is monitored.	Are security violations and activities, including failed logon attempts, other failed access attempts, and sensitive activity, reported to management and investigated?	Review pertinent policies and procedures. Review security violation reports. Examine documentation showing reviews of questionable activities.
13.3 Suspicious access activity is investigated and appropriate action taken.	Do security managers investigate security violations and report results to appropriate supervisory and management personnel?	Test a selection of security violations to verify that follow-up investigations were performed and to determine what action were taken against the perpetrator



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are appropriate disciplinary actions taken?	Review procedures and interview personnel responsible for monitoring of activity.
	Are violations summarized and reported to senior management?	Interview senior management and personnel responsible for summarizing violations. Review any supporting documentation.
	Are access control policies and techniques modified when violations and related risk assessments indicate that such changes are appropriate?	Review policies and procedures and interview appropriate personnel. Review any supporting documentation.
13.4 Security Surveillance	Is all sensitive activity performed by highly privileged accounts monitored for access and maintenance activity?	Verify that there is an appropriate audit trail produced whenever a highly privileged account is used. There should be a traceable trouble ticket opened for each usage and associated audit trail logs outlining the use and appropriate signatures showing concurrence for the use.
Datascope and Sniffers		
14. Network Monitoring	Is software sniffer technology in use?	Determine local policies. If in violation, record an issue.
	Are there procedures governing the use of hardware sniffers and/or datascope?	Obtain procedures and determine whether controls are included by answer the following several questions.
	Does management on a daily basis to ensure usage is justified review the log or audit trail?	For the samples previously selected, verify that a management review was performed.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
Hub Management		
15. Hub Management	Has a management tool been installed on all Hubs?	Verify that SPEL, HUB management tool has been installed.
	Is “Security” turned “On” for all ports on each HUB’s? Configure Hubs with X-disabled ports; X-Send Trap; X-Lock Ports; Define MAC address on all HUB ports?	Ensure that “Security” has been turned “On” for all ports on all HUB’s. Configuration must have the following settings: X-disabled ports; X-Send Trap; X-Lock Ports; Define MAC address on all HUB ports.
	Is a process in place to update HUB inventory?	Verify if HUB inventory process has been developed and implemented.
	Is inventory in place for all physical Hubs and configured ports?	Verify inventory list for all Hubs and check active ports.
Voice Operations		
16.1 System-Related	Are maintenance ports configured to prevent direct access from an external line? This would prevent a hack into the PBX.	Obtain the PBX configuration listing. In addition, try to access the maintenance ports from an outside line. If answer is no, record as comment.
	Are lines that are used for maintenance ports configured through a central office and do they have a different prefix than the regular phone numbers?	Obtain a listing of the maintenance ports modem numbers. If numbers have the same prefix, record as a comment. Review modem technical description and access line information.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	<p>Is invalid access to the maintenance ports tracked and reviewed on a real-time basis? Access to maintenance ports provides the greatest level of access to the system and offers the most potential for abuse.</p>	<p>If system has been outsourced, obtain letter from vendor and vendor's process/ Procedure for performing this function. If system is not outsourced and answer is no, record as a comment. Review PBX maintenance and monitoring procedures.</p>
	<p>Is there a process to ensure that all systems are backed up at a minimum of every 30 days and does it include:</p> <ul style="list-style-type: none">■ Backup whenever a major system reconfiguration is completed.■ (2) copies of backup made with one stored onsite and one offsite?■ Backup Tapes are write protected.	<p>If no, record as comment. Review Copy of process and procedures.</p>
16.2 Maintenance Functions	<p>Is access to the maintenance function limited to administrators on a need to have basis? Unauthorized access to this function can compromise the switch parameters to potential hacking activity.</p>	<p>If outsourced, answer with N/A. If not outsourced, obtain a listing of PBX maintenance users and verify that access is essential. If answer is no, record as a comment. Request a copy of vendor certifications of training.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Do all PBX administrators have their own maintenance ID's and pass-words and are they certified for access to the switch by the vendor? Untrained/uncertified administrators can provide the potential for unwanted parameters leading to potential incidents of toll fraud.	If answer is no, record as a comment.
	Are all administration/ maintenance terminals providing access to telephone system secured at all times? Are terminals logged off when left attended?	
	Is there a process for HR to notify site management of terminated/resigned employees? This is necessary in order to notify the appropriate management of accounts (voice mail and telephone) which need to be terminated.	Check procedure and verify documentation is received of terminated and/or resigned employees. If not, record as comment and obtain procedures of how management is notified. Request listing from HR and sampling of activity for terminated employees.
16.3 Trunking Configuration	Is trunking feature "trunk-to-trunk" activated?	If answer is yes , record as a comment. If yes, review the procedures for managing trunk-to-trunk. Review PBX Configuration printout



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are trunk access codes (TAC) disabled and only enabled for testing purposes, including TAC access to Tie Trunks (if more than one PBX in complex)?	Allowing TAC access to tie trunks on your switch may give the caller access to the Trunk Verification feature on the switch. If not properly administered, a caller may be able to dial 9 or the TAC's in the other switch. Toll hackers can choose a menu option that allows an extension number that provides access to an outside line. Check the PBX configuration files for the presence of Trunk Access <i>Codes</i> . If answer is no, record as comment.
	Is all Direct Inward System Access (DISA) that allows an external caller to gain access to the PBX system features or trunks, functionality disabled? Remote access to these features may result in toll fraud and system abuse.	Check the Class of Service (COS) to verify that DISA is disabled. If answer is no, record as comment. For Lucent Definity G3 type switches, the COS table will have no reference to DISA, UNLESS it is enabled.
	Is access to any known "pay per call" service restricted (i.e., 900, 976, selected 809)? Access to these numbers may cause unwarranted or fraudulent charges.	Check the ARS Table to verify that the numbers are restricted. If the answer is no, record as comment.
	Does the PBX, except for COB purposes restrict codes used for alternate long distance carriers? If not controlled, hackers can dial out by using carrier codes that bypass touting restrictions placed on primary carrier.	Check the PBX configuration files for long distance carrier restrictions. If answer is no, record as comment.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is the PBX set up so that the long distance carrier of choice (e.g. AT&T in the US) is the primary carrier for all long distance calls? And are secondary carriers only used in the event of an outage of the primary carrier.	Obtain telephone bills and verify that no calls are charged except for a MCI (example) emergency. If answer is no, record as comment.
16.4 Class of Service (COS)/Class of Restriction (COR) Configuration	Do semi-annual reviews of the COS levels and CORs take place in light of changing business requirements, improved carrier services, system usage, and organizational re-engineering? This is necessary to insure that excessive entitlements do not exceed requirements of business, resulting in conditions that may lead to system abuse.	Select a sample of added, changed and deleted subscribers and verify procedures are being followed and executed in a satisfactory and timely manner. Determine date of last review of CORs and COS with business and verify review. If answer is no, record as comment.
	Is external call forwarding disabled from all COSs, including Fax Machine/Modem COS? This prevents a user from forwarding an extension to an outside number.	Check the COS to verify that internal call forwarding is allowed. In addition, test the controls by trying to call forward a phone to an outside number. If answer is no, record as comment.
	Are Privileged Abbreviated Dialing Group Lists present on the PBX? These numbers can be used to bypass any COS restrictions and should be restricted to only authorized business related numbers.	Check the PBX configuration files for the presence of speed dialing numbers. If answer is yes, record as comment.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Is access to the outside operator (0, 00, 01, 011, 411, 1411, 611, 1611, 555-1212, and xxx-555-1212) restricted? This is to prevent an operator from connecting a call through to another number.	Check the Class of Service (COS) tables, Class of Restriction (COR), Automatic Route Selection (ARS) Tables, and the Facility Restriction Levels (FRL's) to verify that operator access is not allowed. If present, record as comment.
	Are publicly-accessible phones restricted as follows: <ul style="list-style-type: none">■ to placing only internal, free local, toll-free, and 911 calls■ Call-forwarding deactivated?	If answer is no, record as comment.
	Are publicly-accessible phones used to request admittance into a secured area restricted as follows: <ul style="list-style-type: none">■ to placing 911 and internal calls■ Call-forwarding deactivated?	If answer is no, record as comment.
	Is long distance dialing capability restricted during off-hours? This is a prime time for hackers and other users to abuse the system.	If no, record as comment.
	Are calling cards or authorization codes used after-hours for long distance access if the area in question is not a 24-hour operation?	If no, record as comment.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
16.5 Authorization Codes	Are authorization codes printed in CDR by employee number? If obtained by unauthorized personnel would authorization codes open up those codes to toll fraud?	If listed in CDR by authorization number list as comment.
	Are group accounts or generic account authorization numbers used for visitors? Generic or group accounts prevent accountability by individuals of toll charges.	If yes, list as comment as the CDR report could not identify individual's long distance charges.
	<p>Are there procedures for managing Authorization (Auth) Codes assigned within system? Do they cover the following items:</p> <ul style="list-style-type: none">■ All domestic long distance and international calls require an Auth Code.■ Auth Codes are disabled and new code issued when compromise is suspected and/or confirmed.■ Auth Codes disabled when employee/temp, etc., leaves the bank or relocates to another location.■ Auth Codes must be hand-delivered or sent through registered mail to requesting party, not sent through e-mail, interoffice mail, delivered via telephone, etc.■ No "spare" Auth codes are to be activated.	If no, list as comment.



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
16.6 Call Management System	<p>Is there a process to manage changes to the CMS system that contain:</p> <ul style="list-style-type: none">■ Only system administrator or back-up control all write access to VDN's, vectors, and splits.■ CMS system is partitioned to allow this level of control.■ Deviations are on file for those areas requiring write access to these features and are renewed yearly.	<p>If CMS is installed and answer is no, record comment. Review copy of CMS procedures, configuration and identify deviations.</p>
16.7 Voice Mail System	<p>Does the Voice Mail system require an 8-digit password/pin? Voice mail accounts must be password protected to prevent unauthorized access to user voice mail system.</p>	<p>Obtain the Voice mail configuration file printout and verify. If answer is no, record as a comment.</p>
	<p>Does the Voice mail system disconnect a caller attempting to access the system after 3 invalid PIN attempts are made (within 1 hour for Octel Voice Mail Systems)? If fraudulent use is suspected, notify vendor and insure SDT is notified when the mailbox is disabled.</p>	<p>Test the feature by trying to log in with 3 successive invalid PIN's. If unauthorized access is suspected, notify vendor and await assurance that box has been disabled.</p>



ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are new Voice mail accounts set up with an initial PIN which is unique and which is not the same as the individuals phone extension?	Review the Voice Mail configuration procedures for PIN initialization procedures. If no procedures exist, ask the Voice Mail technician. Test new mailboxes by attempting to access with extension number. If voice mailbox can be accessed, record as comment.
	Does the Voice mail system prohibit external call capability? This prevents a caller from dialing out through the PBX, thus causing Citibank to pick up the tab for long distance calls. (Except on Octel Voice Mail Systems for Citifax, Pager Notification and Voice Mail System Networking)	Obtain the Voicemail configuration file printout and verify. If answer is no, record as comment.
	Does the Voice mail system detect uninitialized mailboxes? And does the system manager remove them after 45 days?	Review site's procedures for uninitialized mailboxes. If answer is no, record as comment.
16.8 Call Detail Reporting System	Is there a Call detail reporting system installed to keep track of length of calls and designation?	If answer is no, record as comment. Review Call detail report & configuration
	Is the CDR system logging and tracking for adequacy the following: <ul style="list-style-type: none">■ all calls over 15 minutes■ Off hour and holiday usage■ Calls over certain dollar amounts	If answer is no, record as comment.



CIAO

ACCESS CONTROLS

Control Objectives	Control Technique	Compliance Procedures
	Are CDR reports reviewed by management every month or whenever an apparent problem occurs (i.e., sudden increase in the number of calls)? Would failure to provide supported businesses with CDR reports disable businesses with a prime management tool to control costs and prevent possible fraud or system abuse?	Obtain copies of old reports and look for signoff. If no, record as comment.
	Does a Contingency plan exist for the PBX? Does it address the issues outlined in the Continuity of Services and Operations questionnaire?	If no, record as comment. Review copy of site COB Plan
	Are Emergency Bypass Phones installed at site and are they installed as follows: <ul style="list-style-type: none">■ Phones are connected to non-PBX lines, i.e., CO/DOD, 1FB/1MB, or Centrex lines.■ Allow full range of out-dial access except for 900, 976 and international calling.	If no, record as comment. Review copy of Emergency Bypass Phone configuration, including location of all phones, and procedures.
16.9 Miscellaneous	Is there a process for producing and reviewing system error reports and logs for: <ul style="list-style-type: none">■ Review on daily basis■ Unauthorized access attempts.■ Multiple invalid password attempts.■ High rates of usage.	If no, record as comment.
16.10 Policies & Procedures	Is an up-to-date Voice Policy and Procedure Manual (PCM) in place and in use?	Check the Voice PCM and insure policies and required reviews are up to date.



CIAO

**Appendix C:
Segregation of Duties**

Control Objectives	Control Technique	Compliance Procedures
Policies		
1.1 Incompatible duties have been identified and policies implemented to segregate these duties.	Do policies and procedures exist for segregating duties? If so, are they up-to-date?	Review pertinent policies and procedures. Interview selected management and IS personnel regarding segregation of duties.
	Are distinct systems support functions performed by different individuals, including the following? <ul style="list-style-type: none">■ IS management■ System design■ Application programming■ Systems programming■ Quality assurance/testing■ Library management and change management■ Computer operations■ Production control and scheduling■ Data control■ Data security■ Data administration	Review an agency organization chart showing IS functions and assigned personnel. Interview selected personnel and determine whether functions are appropriately segregated. Determine whether the chart is current and different individuals staff each function. Review relevant alternate or backup assignments and determine whether the proper segregation of duties is maintained. Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.



SEGREGATION OF DUTIES

Control Objectives	Control Technique	Compliance Procedures
	<p>Do any individuals have complete control over incompatible transaction processing functions? Specifically, are the following combinations of functions performed by a single individual?</p> <ul style="list-style-type: none">■ Data entry and verification of data■ Data entry and its reconciliation to output■ Input of transactions for incompatible processing functions (e.g. input of vendor invoices, and purchasing and receiving information)■ Data entry and supervisory override functions(e.g., authorizing a rejected transaction to continue processing that exceeds some limit requiring a supervisor's review and approval)	<p>Review the organizational chart and interview personnel to determine that assignments do not result in a single person being responsible for the indicated combinations of functions.</p> <p>Observe activities of personnel to determine the nature and extent of the compliance with the intended segregation of duties.</p>
	<p>Are data processing personnel also users of information systems? Do data processing personnel or security managers initiate, input, or correct transactions?</p>	<p>Determine through interview and observation whether data processing personnel and security managers are prohibited from these activities.</p>
	<p>Are day-to-day operating procedures for the data center adequately documented and are prohibited actions identified?</p>	<p>Review the adequacy of documented operating procedures for the data center.</p>



SEGREGATION OF DUTIES

Control Objectives	Control Technique	Compliance Procedures
	Do departures from standard job schedules occur?	Review procedures that identify, investigate, and approve departures from standard job schedules.
	Are regularly scheduled vacations and periodic job/shift rotations required (see SP-4.1 on personnel policies)?	Individuals performing incompatible duties and conducting inappropriate actions could be detected when another individual undertakes those duties. Requiring vacations and rotations helps detect such actions.
	Do documented job descriptions include definitions of the technical knowledge, skills, and abilities required for successful performance in the relevant position, and can they be used for hiring, promoting, and performance evaluation purposes?	Review job descriptions and interview management personnel.
1.2 Employees understand their duties and responsibilities.	Do all employees fully understand their duties and responsibilities, and carry out those responsibilities in accordance to their job descriptions?	Interview personnel filling positions for the selected job descriptions (see above). Determine if the descriptions match their understanding of their duties and responsibilities and whether additional duties are undertaken that are not reflected in their job descriptions.
	Is senior management responsible for providing adequate resources and training in assuring that segregation of duty principles are understood and established, enforced, and institutionalized within the organization?	Determine from interviewed personnel whether senior management has provided adequate resources and training to establish, enforce, and institutionalize the principles of segregation of duties.



SEGREGATION OF DUTIES

Control Objectives	Control Technique	Compliance Procedures
	Are responsibilities for restricting access by job positions in key operating and programming activities clearly defined, understood, and followed?	Interview management personnel in these activities.
Access Controls to Enforce Segregation of Duties		
2. Establish access controls to enforce segregation of duties	Are management reviews performed to determine that control techniques for segregating incompatible duties are functioning as intended and that the control techniques in place are maintaining risks within acceptable levels (e.g., periodic risk assessments)?	Determine what reviews are conducted to assess the adequacy of duty segregation. Obtain and review results of such reviews.
Operating Procedures, Supervision, and Review		
3.1 Formal procedures provide guidance for the performance of personnel activities	Do detailed, written instructions exist and are they followed for the performance of work?	Review manuals. Interview supervisors and personnel. Observe processing activities.
	Do operator instruction manuals provide guidance on system operation?	Review manuals.
	Do application run manuals provide instruction on operating specific applications?	Review manuals.
	Are operators prevented from overriding file label or equipment error messages?	Interview supervisors and personnel.



SEGREGATION OF DUTIES

Control Objectives	Control Technique	Compliance Procedures
3.2 Active supervision and review are provided for all personnel	Are personnel provided adequate supervision and review, including each shift for computer operations?	Interview supervisors and personnel Observe processing activities. Review history log reports for signatures indicating supervisory review. Determine who is authorized to IPL the system, what steps are followed, and what controls are in place to monitor console activity during the process. Determine whether operators override the IPL parameters.
	Are all operator activities on the computer system recorded on an automated history log?	Interview management. Review history logs.
	Is system startup monitored and performed by authorized personnel? Are parameters set during the initial program load (IPL) in accordance with established procedures?	Interview management and subordinate staff. Review procedures that identify the tasks associated with documenting, periodically testing, and adjusting start-up processes.



Appendix D: Continuity of Services and Operations

Control Objectives	Control Technique	Compliance Procedures
Business Continuity Plan		
1.1 Resources supporting critical operations are identified.	Have resources supporting critical operations been identified and documented? Do identified resources include: <ul style="list-style-type: none">■ computer hardware,■ computer software,■ computer supplies,■ system documentation,■ telecommunications,■ office facilities and supplies, and■ human resources?	Review related documentation. Interview program and security administration officials.
1.2 Critical Information Technology Resources are identified.	Does the continuity plan identify the critical application programs, third-party services, operating systems, personnel and supplies, data files and time frames needed for recovery after a disaster occurs?	Review BCP
1.3 Availability Plan.	Does senior management concerning the availability of data processing and on-line services establish goals?	Interview senior management, data processing management, and user management. Review supporting documentation.
	Has management established an availability plan to achieve, monitor and control the availability of information services?	Obtain and review minutes of meetings discussing capacity planning and performance measurement



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
1.4 EMERGENCY PROCESSING PRIORITIES ARE ESTABLISHED.	HAVE EMERGENCY PROCESSING PRIORITIES BEEN DOCUMENTED AND APPROVED BY APPROPRIATE PROGRAM AND DATA PROCESSING MANAGERS?	REVIEW RELATED POLICIES. REVIEW RELATED DOCUMENTATION. Interview program and security administration officials.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
1.5 Information Technology Continuity Plan Contents	<ul style="list-style-type: none">■ Does the Continuity of Service Plan contain the following:■ Guidelines on how to use the continuity plan;■ Emergency procedures to ensure the safety of all affected staff members;■ Response procedures meant to bring the business back to the state it was in before the incident or disaster;■ Recovery procedures meant to bring the business back to the state it was in before the incident or disaster;■ Procedures to safeguard and reconstruct the home site;■ Co-ordination procedures with public authorities;■ Communication procedures with stakeholders: employees, key customers, critical suppliers, stockholders and management; and■ Critical information on continuity teams, affected staff, customers, suppliers, public authorities and media?	Review BCP



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
1.6 MAINTAINING THE INFORMATION TECHNOLOGY CONTINUITY PLAN	ARE THERE, IN THE BCP, CHANGE CONTROL PROCEDURES ENSURING THAT THE CONTINUITY PLAN IS UP-TO-DATE AND REFLECTS ACTUAL BUSINESS REQUIREMENTS?	REVIEW BCP
1.7 INFORMATION TECHNOLOGY CONTINUITY PLAN DISTRIBUTION	GIVEN THE SENSITIVE NATURE OF INFORMATION IN THE CONTINUITY PLAN, IS THE BCP DISTRIBUTED ONLY TO AUTHORIZED PERSONNEL AND SHOULD BE SAFE-GUARDED AGAINST UNAUTHORIZED DISCLOSURE. CONSEQUENTLY, SECTIONS OF THE PLAN NEED TO BE DISTRIBUTED ON A NEED- TO-KNOW BASIS?	REVIEW BCP
1.8 INFORMATION TECHNOLOGY CONTINUITY PLAN TRAINING	DOES THE DISASTER CONTINUITY METHODOLOGY ENSURE THAT ALL CONCERNED PARTIES RECEIVE REGULAR TRAINING SESSIONS REGARDING THE PROCEDURES TO BE FOLLOWED IN CASE OF AN INCIDENT OR DISASTER?	REVIEW BCP
1.9 TESTING THE INFORMATION TECHNOLOGY CONTINUITY PLAN	DOES MANAGEMENT ASSESS THE ADEQUACY OF TEST RESULTS?	REVIEW BCP TESTING PROCEDURES



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ON SUCCESSFUL RESUMPTION OF THE INFORMATION SERVICES FUNCTION AFTER A DISASTER OR A TEST, HAS MANAGEMENT ESTABLISHED PROCEDURES FOR ASSESSING THE ADEQUACY OF THE PLAN AND UPDATING THE PLAN ACCORDINGLY.	REVIEW BCP & RESULTS OF RECENT TEST OR DISASTER. NOTE ANY CORRECTIVE ACTIONS AND MODIFICATIONS TO PLAN TO INCORPORATE THEM.
Resource Management - COB		
2.1 MANAGE PERFORMANCE AND CAPACITY	THE MANAGEMENT PROCESS SHOULD ENSURE THAT BUSINESS NEEDS ARE IDENTIFIED REGARDING AVAILABILITY AND PERFORMANCE OF INFORMATION SERVICES AND CONVERTED INTO AVAILABILITY TERMS AND REQUIREMENTS.	ANALYSIS SHOULD BE CONDUCTED ON SYSTEM FAILURES AND IRREGULARITIES PERTAINING TO FREQUENCY, DEGREE OF IMPACT AND AMOUNT OF DAMAGE.
	DOES THE PERFORMANCE MANAGEMENT PROCESS INCLUDE FORECASTING CAPABILITY TO ENABLE PROBLEMS TO BE CORRECTED BEFORE THEY AFFECT SYSTEM PERFORMANCE?	REVIEW THE PERFORMANCE MANAGEMENT PROCESS.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
2.2 WORKLOAD FORECASTING	ARE CONTROLS IN PLACE TO ENSURE THAT WORKLOAD FORECASTS ARE PREPARED TO IDENTIFY TRENDS AND TO PROVIDE INFORMATION NEEDED FOR THE CAPACITY PLAN?	OBTAIN AND ANALYZE TREND ANALYSIS REPORTS.
2.3 CAPACITY MANAGEMENT OF RESOURCES	IS THERE A PLANNING PROCESS FOR THE REVIEW OF HARDWARE PERFORMANCE AND CAPACITY TO ENSURE THAT COST-JUSTIFIABLE CAPACITY ALWAYS EXISTS TO PROCESS THE AGREED WORKLOADS AND TO PROVIDE THE REQUIRED PERFORMANCE QUALITY AND QUANTITY PRESCRIBED IN SERVICE LEVEL AGREEMENTS?	REVIEW PROCEDURES AND CAPACITY STUDIES.
	ARE FAULT TOLERANCE MECHANISMS, PRIORITIZING TASKS AND EQUITABLE RESOURCE ALLOCATION MECHANISMS IN USE?	REVIEW FAULT TOLERANCE MECHANISMS IN USE.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	HAS MANAGEMENT ENSURED THE TIMELY ACQUISITION OF REQUIRED CAPACITY, TAKING INTO ACCOUNT ASPECTS SUCH AS RESILIENCE, CONTINGENCY, WORKLOADS AND STORAGE PLANS.	REVIEW CAPACITY AND RESOURCE PLANS AND WORKLOAD PLANNING DOCUMENTS. REVIEW RESULTS OF CONTINGENCY TESTS.
2.4 SYSTEM MAINTENANCE IS PERFORMED WITH THE LEAST AMOUNT OF IMPACT.	IS ADVANCE NOTIFICATION ON HARDWARE CHANGES GIVEN TO USERS SO THAT SERVICE IS NOT UNEXPECTEDLY INTERRUPTED?	REVIEW HARDWARE CHANGE PROCEDURE
	IS ROUTINE PERIODIC HARDWARE PREVENTATIVE MAINTENANCE SCHEDULED AND PERFORMED IN ACCORDANCE WITH VENDOR SPECIFICATIONS, AND IN A MANNER THAT MINIMIZES THE IMPACT ON OPERATIONS?	INTERVIEW DATA PROCESSING AND USER MANAGEMENT. REVIEW MAINTENANCE DOCUMENTATION.
	IS REGULAR AND UNSCHEDULED MAINTENANCE PERFORMED AND DOCUMENTED?	CHECK MAINTENANCE PROCEDURES AND MAINTENANCE LOGS.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
2.5 ENSURE CONTINUOUS SERVICE	INFORMATION SERVICES FUNCTION MANAGEMENT IS TO CREATE A CONTINUITY FRAMEWORK WHICH DEFINES THE ROLES, RESPONSIBILITIES, THE RISK BASED APPROACH/METHODOLOGY TO BE ADOPTED, AND THE RULES AND STRUCTURES TO DOCUMENT THE PLAN AS WELL AS THE APPROVAL PROCEDURES.	REVIEW THE CONTINUITY FRAMEWORK. REVIEW THE RULES AND STRUCTURES USED TO DOCUMENT THE COB PLAN. REVIEW THE APPROVAL PROCEDURES.
	HAS THE BUSINESS UNIT HEAD APPOINTED A RESPONSE TEAM TO COORDINATE RECOVERY ACTIONS DURING AND AFTER A CONTINGENCY?	IF YES VERIFY THAT THE RESPONSE TEAM IS PART OF THE ANNUAL CONTINGENCY TEST.
	DOES THE COB PLAN INCLUDE PROCEDURES ON HOW TO ALERT INDIVIDUALS ON WHERE TO GO IN CASE OF A CONTINGENCY?	IF YES, VERIFY THOSE UPDATED MAPS, TRAVEL INFORMATION, AND ESCALATION PLANS ARE INCLUDED IN THE COB.
	DOES THE COB PLAN CALL FOR ALL ASSOCIATED BUSINESS UNITS TO BE ALERTED TO ANY DEFICIENCIES IN THE CONTINGENCY PROCESS?	IF YES, ASK FOR AND REVIEW ANY ALERT MESSAGES ASSOCIATED WITH FAILED OR DEFICIENT PARTS OF THE PLAN AND TESTING PROCESS AND VERIFY THAT ALL BUSINESS WERE NOTIFIED.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
2.6 INFORMATION TECHNOLOGY CONTINUITY PLAN	MANAGEMENT SHOULD ENSURE THAT THE INFORMATION TECHNOLOGY CONTINUITY PLAN IS IN LINE WITH THE OVERALL BCP TO ENSURE CONSISTENCY.	INTERVIEW SENIOR MANAGEMENT.
2.7 ENSURE BUSINESS REVIEW OF CONTINUITY OF BUSINESS (COB) PLAN	HAS THE COB PLAN BEEN REVIEWED BY THE BUSINESS HEAD ON AN ANNUAL BASIS OR AFTER A MAJOR CHANGE HAS OCCURRED?	VERIFY THE COB PLAN CONTAINS A SECTION SHOWING THE PROPER BUSINESS SIGNOFFS SHOWING PLAN ACCEPTANCE.
	IS THE COB PLAN REVIEWED AT LEAST SEMI- ANNUALLY BY A RESPONSIBLE PERSON TO VERIFY THAT ALL SECTIONS ARE UP TO DATE (E.G. PERSONNEL, PHONE NUMBERS, SITES)?	VERIFY THE COB PLAN CONTAINS A SECTION SHOWING SIGNATURE OF PERSON WHO UPDATED THE PLAN.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
Contingency Plan		



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
3.1 AN UP-TO-DATE CONTINGENCY PLAN IS DOCUMENTED.	HAS A CONTINGENCY PLAN BEEN DOCUMENTED THAT: <ul style="list-style-type: none">■ REFLECTS CURRENT CONDITIONS,■ THAT HAS BEEN APPROVED BY KEY AFFECTED GROUPS, INCLUDING, SENIOR MANAGEMENT, DATA CENTER MANAGEMENT, AND PROGRAM MANAGERS,■ CLEARLY ASSIGNS RESPONSIBILITIES FOR RECOVERY,■ INCLUDES DETAILED INSTRUCTIONS FOR RESTORING OPERATIONS (BOTH OPERATING SYSTEM AND CRITICAL APPLICATIONS),■ IDENTIFIES THE ALTERNATE PROCESSING FACILITY AND THE BACK-UP STORAGE FACILITY,■ INCLUDES PROCEDURES TO FOLLOW WHEN THE DATA/SERVICE CENTER IS UNABLE TO RECEIVE OR TRANSMIT DATA,■ IDENTIFIES CRITICAL DATA FILES,■ IS DETAILED ENOUGH TO BE UNDERSTOOD BY ALL AGENCY MANAGERS,■ INCLUDES	REVIEW THE CONTINGENCY PLAN AND COMPARE ITS PROVISIONS WITH THE MOST RECENT RISK ASSESSMENT AND WITH A CURRENT DESCRIPTION OF AUTOMATED OPERATIONS. INTERVIEW SENIOR MANAGEMENT, DATA CENTER MANAGEMENT, AND PROGRAM MANAGERS.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
3.2 CONTINGENCY PLAN ADDRESSES ALL COMPONENTS.	IS SPARE OR BACKUP HARDWARE USED TO PROVIDE A HIGH LEVEL OF SYSTEM AVAILABILITY FOR CRITICAL AND SENSITIVE APPLICATIONS?	INTERVIEW DATA CENTER MANAGEMENT.
	DOES THE PLAN PROVIDE FOR BACKUP PERSONNEL SO THAT IT CAN BE IMPLEMENTED INDEPENDENT OF SPECIFIC INDIVIDUALS?	REVIEW THE CONTINGENCY PLAN.
	HAVE USER DEPARTMENTS DEVELOPED ADEQUATE MANUAL/PERIPHERAL PROCESSING PROCEDURES FOR USE UNTIL OPERATIONS ARE RESTORED?	INTERVIEW SENIOR MANAGEMENT, DATA CENTER MANAGEMENT, AND PROGRAM MANAGERS.
	ARE SEVERAL COPIES OF THE CURRENT CONTINGENCY PLAN SECURELY STORED OFF- SITE AT DIFFERENT LOCATIONS?	OBSERVE COPIES OF THE CONTINGENCY PLAN HELD OFF-SITE.
	IS THE CONTINGENCY PLAN PERIODICALLY REASSESSED AND, IF APPROPRIATE, REVISED TO REFLECT CHANGES IN HARDWARE, SOFTWARE, AND PERSONNEL?	REVIEW THE PLAN AND ANY DOCUMENTATION SUPPORTING RECENT PLAN REASSESSMENTS.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
3.3 THE PLAN IS PERIODICALLY TESTED.	HAS THE CURRENT PLAN BEEN TESTED UNDER CONDITIONS THAT SIMULATE A DISASTER?	REVIEW POLICIES ON TESTING. REVIEW TEST RESULTS. OBSERVE A DISASTER RECOVERY TEST.
	HAVE TEST RESULTS BEEN DOCUMENTED AND HAS A REPORT, SUCH AS A “LESSONS LEARNED” REPORT, BEEN DEVELOPED AND PROVIDED TO SENIOR MANAGEMENT?	REVIEW FINAL TEST REPORT. INTERVIEW SENIOR MANAGERS TO DETERMINE IF THEY ARE AWARE OF THE TEST RESULTS.
	WERE THE CONTINGENCY PLAN AND RELATED AGREEMENTS AND PREPARATIONS ADJUSTED TO CORRECT ANY DEFICIENCIES IDENTIFIED DURING TESTING?	REVIEW ANY DOCUMENTATION SUPPORTING CONTINGENCY PLAN ADJUSTMENTS.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
Service Level Agreement Management		
4.1 SERVICE LEVEL AGREEMENT FRAMEWORKS ARE ESTABLISHED	HAS SENIOR MANAGEMENT DEFINED A FRAMEWORK WHEREIN IT PROMOTES THE DEFINITION OF FORMAL SERVICE LEVEL AGREEMENTS AND DEFINED THE MINIMAL CONTENTS?	REVIEW SERVICE LEVEL AGREEMENTS. USERS AND THE INFORMATION SERVICES FUNCTION SHOULD HAVE A WRITTEN AGREEMENT, WHICH DESCRIBES THE SERVICE LEVEL IN QUALITATIVE AND QUANTITATIVE TERMS. THE AGREEMENT DEFINES THE RESPONSIBILITIES OF BOTH PARTIES. THE INFORMATION SERVICES FUNCTION MUST OFFER THE AGREED QUALITY AND QUANTITY OF SERVICE AND THE USERS MUST CONSTRAIN THE DEMANDS THEY PLACE UPON THE SERVICE WITHIN THE AGREED LIMITS.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
4.2 ASPECTS OF SERVICE LEVEL AGREEMENTS	DO THE SERVICE LEVEL AGREEMENTS COVER, AT LEAST, THE FOLLOWING ASPECTS: AVAILABILITY, RELIABILITY, PERFORMANCE, CAPACITY FOR GROWTH, LEVELS OF SUPPORT PROVIDED TO USERS, CONTINUITY PLANNING, SECURITY, MINIMUM ACCEPTABLE LEVEL OF SATISFACTORILY DELIVERED SYSTEM FUNCTIONALITY, RESTRICTIONS (LIMITS ON THE AMOUNT OF WORK), SERVICE CHARGES, CENTRAL PRINT FACILITIES (AVAILABILITY), CENTRAL PRINT DISTRIBUTION AND CHANGE PROCEDURES?	REVIEW SERVICE LEVEL AGREEMENTS AND PERFORMANCE TRACKING MEASURES.
4.3 PERFORMANCE PROCEDURES	ARE PROCEDURES IN PLACE TO ENSURE THAT THE MANNER OF AND RESPONSIBILITIES FOR PERFORMANCE GOVERNING RELATIONS (E.G., NON-DISCLOSURE AGREEMENTS) BETWEEN ALL INVOLVED PARTIES ARE ESTABLISHED, COORDINATED, MAINTAINED AND COMMUNICATED TO ALL AFFECTED DEPARTMENTS?	OBTAIN EVIDENCE OF LEGAL REVIEW/APPROVAL OF THE CONTRACT



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
4.4 MONITORING AND REPORTING	ARE SERVICE FUNCTIONS MONITORED BY A SERVICE LEVEL MANAGER WHO IS RESPONSIBLE FOR MONITORING AND REPORTING ON THE ACHIEVEMENT OF THE SPECIFIED SERVICE PERFORMANCE CRITERIA AND ALL PROBLEMS ENCOUNTERED DURING PROCESSING?	REVIEW PERFORMANCE-TRACKING METHODS. THE MONITORING STATISTICS SHOULD BE ANALYZED ON A TIMELY BASIS. APPROPRIATE CORRECTIVE ACTION SHOULD BE TAKEN AND FAILURES SHOULD BE INVESTIGATED.
4.5 REVIEW OF SERVICE LEVEL AGREEMENTS AND CONTRACTS	DOES MANAGEMENT PERFORM A REGULAR REVIEW PROCESS FOR SERVICE LEVEL AGREEMENTS AND UNDERPINNING CONTRACTS WITH THIRD-PARTY SERVICE PROVIDERS?	OBTAIN EVIDENCE OF REVIEW.
Data Center Management		
5.1 ORGANIZATION OF DATA CENTER	ARE THE EQUIPMENT LAYOUT DESIGNS (FLOOR PLANS) CURRENT?	OBTAIN FLOOR PLANS.
	ARE CABINETS/FRAMES SPACED SO THAT EQUIPMENT IS A MINIMUM OF 36" FROM THE BACK WALLS OR FROM THE NEXT BANK OF CABINETS/FRAMES?	VERIFY THAT EQUIPMENT IS SPACED PROPERLY EITHER THROUGH MEASUREMENT OR THROUGH FLOOR PLAN,



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE ALL SYSTEMS LABELED TO ASSURE PROPER USAGE (E.G., ROUTER NAME, IP ADDRESS, NODE NAME, ETC.)?	PERFORM WALKTHROUGH AND SELECT CERTAIN EQUIPMENT AND VERIFY ACCURACY OF LABELS.
	IS ALL EQUIPMENT (E.G., PORTS, PATCH PANELS) AND CABLES PROPERLY LABELED END TO END?	SELECT VARIOUS EQUIPMENT TYPES (PORTS, PATCH PANELS, ETC.) AND CABLES AND VERIFY THE ACCURACY OF THE LABELS.
	DOES THE SITE HAVE PROCEDURES FOR PREPARING FOR THE SHUTDOWN AND START-UP OF EQUIPMENT DURING REGULARLY SCHEDULED BUILDING POWER OUTAGES?	OBTAIN PROCEDURES AND DETERMINE WHETHER ALL TYPES OF EQUIPMENT ARE ADDRESSED. IN MANY CASES, EQUIPMENT MUST BE BROUGHT DOWN AND UP GRADUALLY SO AS NOT TO CAUSE ADDITIONAL PROBLEMS.
	IS UPS INSTALLED ON KEY EQUIPMENT?	OBTAIN A LIST OF EQUIPMENT ON UPS. DETERMINE WHETHER THE LIST IS COMPREHENSIVE ENOUGH.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	DO PROCEDURES EXIST TO PERIODICALLY TEST THE UPS EQUIPMENT AND ARE THEY BASED ON THE MANUFACTURER'S RECOMMENDATIONS?	OBTAIN UPS TEST PROCEDURES. VERIFY THAT TESTING FREQUENCY IS ADEQUATE, BASED ON MANUFACTURER'S INSTRUCTIONS. VERIFY TESTS WERE PERFORMED ACCORDING TO THAT FREQUENCY.
	ARE UPS BATTERIES CHECKED TO ENSURE THAT THEY WILL FUNCTION PROPERLY IN A CONTINGENCY SITUATION?	OBTAIN PROCEDURES FOR MONITORING BATTERY POWER. MOST BATTERIES ARE ONLY GUARANTEED FOR 5 YEARS AND SHOULD BE CHECKED PERIODICALLY TO AVOID POTENTIAL PROBLEMS DURING POWER OUTAGES.
	IS THE CAPACITY OF THE UPS CHECKED PERIODICALLY?	DETERMINE AMPS NEEDED TO SUPPORT EQUIPMENT. REVIEW TEST RESULTS TO DETERMINE IF NUMBER OF AMPS PROVIDED BY UPS ADDRESSES THE NEED. CHECK WITH BUILDING ENGINEER IF NECESSARY.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	IS UPS BEING CHARGED WHEN THE FACILITY IS OPERATING UNDER BACKUP POWER?	OBTAIN EVIDENCE FROM BUILDING MANAGEMENT THAT UPS IS CHARGED WHILE BACKUP GENERATORS ARE FUNCTIONING, IN ORDER TO AVOID ANY POWER DISRUPTIONS.
	IS THE UPS AUTOMATICALLY SWITCHED TO THE GENERATORS IN THE EVENT OF A POWER OUTAGE?	VERIFY THAT SWITCH IS MADE AUTOMATICALLY EITHER BY REVIEWING TEST RESULTS OR THROUGH INTERVIEWS WITH BUILDING MANAGEMENT.
	ARE GENERATORS IN USE FOR BACKUP POWER FOR THE FACILITY?	DETERMINE EXISTENCE OF SUCH GENERATORS.
	ARE GENERATORS TESTED IN ACCORDANCE WITH MANUFACTURERS' REQUIREMENTS? IS THE TESTING OF BUILDING GENERATORS TIED TO TESTING THE ON-SITE CONTINGENCY REQUIREMENTS OF THE UNIT?	OBTAIN EVIDENCE OF TESTING PERFORMED FROM MANAGEMENT. DETERMINE WHETHER TESTING REQUIREMENTS WERE MET BY REVIEWING MANUFACTURER'S DOCUMENTATION AND HOW TEST RESULTS ARE TIED TO THE COB PLAN.
	IS EMERGENCY LIGHTING IN PLACE IN THE EVENT OF A POWER FAILURE?	PERFORM A WALK-THROUGH TO DETERMINE THE EXISTENCE OF EMERGENCY LIGHTING.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE EMERGENCY EXIT SIGNS LIGHTED BY THEIR OWN POWER?	PERFORM A WALK-THROUGH TO ENSURE THAT EXIT SIGNS WILL BE ILLUMINATED IN THE EVENT OF A POWER FAILURE.
	ARE “EXIT” AND “NO SMOKING” SIGNS VISIBLY POSTED IN THE FACILITY?	PERFORM A WALK-THROUGH OF AREA IN QUESTION. IDENTIFY ALL EXITS AND DETERMINE WHETHER EXIT AND NO SMOKING SIGNS ARE VISIBLE.
	IS THERE AN EMERGENCY POWER CUTOFF SWITCH?	PERFORM A WALK-THROUGH OF AREA. DETERMINE THE EXISTENCE OF SUCH A POWER SWITCH.
	IS THERE A FIRST AID KIT READILY AVAILABLE IN THE FACILITY?	DETERMINE EXISTENCE OF KIT. IF KIT DOES NOT EXIST, THEN RECORD ISSUE.
	ARE EMERGENCY NUMBERS (FIRE, SECURITY, MEDICAL) POSTED IN THE DATA CENTER OR AFFIXED TO ALL PHONES?	PERFORM WALK-THROUGH OF THE AREA. DETERMINE WHETHER EMERGENCY NUMBERS ARE VISIBLE TO PERSONNEL.
	IS THE FACILITY INCLUDING DESKS, MAINTAINED WELL, E.G. NEAT AND CLEAN?	PERFORM A WALK-THROUGH OF THE AREA. DETERMINE WHETHER AREA IS NEAT/CLEAN.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE FORMS, PAPERS, AND OTHER SUPPLIES KEPT TO A MINIMUM AND STORED IN A MANNER THAT DOES NOT REPRESENT A SAFETY HAZARD?	PERFORM A WALK-THROUGH OF THE AREA. DETERMINE WHETHER MATERIALS ARE STORED PROPERLY SO AS NOT TO CAUSE A SAFETY CONCERN.
	IS ALL CABLING ROUTED NEATLY AND TIE-WRAPPED (WITH EXCESS CABLING REMOVED), ESPECIALLY WHERE THERE ARE LARGE PERCENTAGES OF LEGACY EQUIPMENT?	PERFORM A WALK-THROUGH OF THE AREA. THROUGH OBSERVATION, ESTABLISH WHETHER CABLES ARE ROUTED/SECURED PROPERLY.
	IF RAISED FLOORS EXIST IN THE DATA CENTER, IS THE AREA UNDER THE FLOOR INSPECTED MONTHLY AND CLEANED EVERY SIX MONTHS?	IF RAISED FLOORS ARE IN USE, OBTAIN EVIDENCE OF MONTHLY INSPECTION AND CLEANING. IF NECESSARY, PERFORM YOUR OWN INSPECTION.
	IS THERE A FIRE ALARM SYSTEM INSTALLED CONSISTING OF MANUAL AND AUTOMATIC SUB-SYSTEMS?	VERIFY RECORDS FROM MANAGEMENT THAT SYSTEMS ARE INSTALLED.
	IS THE MANUAL FIRE ALARM SYSTEM TESTED QUARTERLY AND THE AUTOMATIC SYSTEM TESTED ANNUALLY BY THE BUILDING/FACILITY?	VERIFY RECORDS FROM MANAGEMENT THAT SYSTEMS WERE TESTED AS REQUIRED.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	DOES THE AUTOMATIC FIRE ALARM SUB-SYSTEM INCLUDE AUTOMATIC DETECTION DEVICES, I.E., SMOKE, HEAT, AND FLAME DETECTORS?	VERIFY RECORDS FROM MANAGEMENT THAT AUTOMATIC FIRE DETECTION DEVICES INCLUDE SMOKE, HEAT, AND FLAME DETECTORS.
	DOES THE FIRE DETECTION SYSTEM SET OFF AN AUDIBLE ALARM IN THE FACILITY/ BUILDING, SECURITY OFFICE AND/OR LOCAL FIRE DEPARTMENT?	DETERMINE THE EXISTENCE OF FIRE ALARM SYSTEMS AND WHETHER ALARM IS AUDIBLE.
	ARE AUTOMATED FIRE SUPPRESSION DEVICES INSTALLED?	ALL FACILITIES MUST HAVE SUPPRESSION DEVICES.
	ARE AUTOMATED FIRE SUPPRESSION DEVICES TESTED EACH YEAR AND IS EVIDENCE OF THIS TESTING MAINTAINED?	VERIFY RECORDS FROM MANAGEMENT THAT DEVICES WERE TESTED ACCORDINGLY.
	ARE FIRE DRILLS CONDUCTED QUARTERLY?	VERIFY THAT FIRE DRILLS WERE CONDUCTED BY INTERVIEWING THE FIRE WARDEN OR TALKING TO BUILDING PERSONNEL.
	ARE THE APPROPRIATE PORTABLE FIRE EXTINGUISHERS INSTALLED (E.G., WATER, FOAM, CO₂) BASED ON THE TYPE OF EQUIPMENT AND MATERIALS IN THE AREA?	DETERMINE THE LOCATION OF EACH PORTABLE FIRE EXTINGUISHER IN THE AREA IN QUESTION AND VERIFY THAT THE RIGHT TYPE OF FIRE EXTINGUISHERS IS PRESENT.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE THE PORTABLE FIRE EXTINGUISHERS CHECKED AT LEAST ANNUALLY OR ACCORDING TO LOCAL CODE (E.G., SOME STATES REQUIRES A SEMI-ANNUAL CHECK)?	CHECK EACH PORTABLE FIRE EXTINGUISHER TO VERIFY THAT AN AUTHORIZED AGENT SERVICED THEM WITHIN THE LAST YEAR.
	IS THE DATA CENTER BELOW GROUND LEVEL WHERE WATER MAY CAUSE A PROBLEM?	EVALUATE THE RISK WITH APPROPRIATE MANAGEMENT.
	IS THERE A MANUAL CUTOFF VALVE FOR WATER PIPES ENTERING THE FACILITY?	DETERMINE THE EXISTENCE OF WATER PIPES EITHER OVERHEAD OR AT GROUND LEVEL OR BELOW. IF PIPES EXIST, DETERMINE WHETHER SUCH A CUTOFF VALVE IS NECESSARY.
	ARE PLASTIC COVERS AVAILABLE TO PROTECT FACILITY EQUIPMENT FROM OVERHEAD WATER LEAKS?	IF PIPES EXIST, DETERMINE WHETHER PLASTIC COVERS EXIST.
	ARE OPENINGS, PIPES, CONDUITS AND CABLES PASSING THROUGH FIREWALLS SEALED TO PREVENT TUNNELING EFFECTS IN CASE OF FIRE?	PERFORM A WALK-THROUGH OF THE AREA. DETERMINE WHETHER SUCH OPENINGS PRESENT ANY HAZARDS.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE WATER DETECTORS INSTALLED?	FIRE/SAFETY STANDARD REQUIRES WATER DETECTORS BE INSTALLED IN EVERY FACILITY.
	ARE EMERGENCY EVACUATION PROCEDURES POSTED IN THE DATA CENTER?	PERFORM A WALK-THROUGH OF THE AREA. DETERMINE EXISTENCE OF SUCH PROCEDURES AND WHETHER OR NOT THEY ARE POSTED.
	ARE EMERGENCY EVACUATION PROCEDURES REVIEWED QUARTERLY WITH THE FIRE WARDEN?	OBTAIN EVIDENCE OF REVIEW FROM MANAGEMENT.
	ARE TRASHCANS IN USE WITHIN EACH FACILITY CONSTRUCTED FROM NON-COMBUSTIBLE MATERIALS WITH A SOLID BOTTOM AND SIDES OR LINED WITH A NON-COMBUSTIBLE MATERIAL?	PERFORM A WALK-THROUGH OF THE AREA. DETERMINE WHETHER TRASHCANS MEET REQUIREMENTS OF THE STANDARD.
	HAVE TEMPERATURE AND HUMIDITY GAUGES BEEN INSTALLED AND ARE THEY BEING MONITORED?	DETERMINE LOCATION OF DEVICES. OBTAIN PROCEDURES FOR MONITORING DEVICES. MAKE SURE THAT DEVICES ARE BEING MONITORED AS REQUIRED. IF DEVICES ARE NOT INSTALLED OR ARE NOT BEING MONITORED.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	IS A/C INSTALLED IN THE DATA CENTER TO ENSURE THAT ROOM TEMPERATURES ARE IN COMPLIANCE WITH MANUFACTURER'S REQUIREMENTS, TO LIMIT DOWNTIME?	DETERMINE IF SEPARATE A/C UNITS ARE NEEDED BASED ON TYPE OF EQUIPMENT IN USE. IF THE BUILDING PROVIDES A/C, ENSURE THAT TEMPERATURES ARE BEING MONITORED AND PRECAUTIONS (E.G., FANS) ARE IN PLACE TO ADDRESS OUTAGES.
	IS THE A/C SERVICED IN ACCORDANCE WITH THE MANUFACTURER'S REQUIREMENTS?	OBTAIN INVOICES OR SERVICE LOGS THAT SEPARATE A/C UNITS WERE SERVICED.
	ARE WATER DETECTORS IN PLACE AROUND STAND-ALONE A/C UNITS?	EITHER THROUGH OBSERVATION OR BY REVIEWING THE FLOOR PLAN, ENSURE THAT WATER DETECTORS ARE IN PLACE AROUND THE A/C UNITS.
	HAVE ALL DATA CENTER EMPLOYEES RECEIVED TRAINING AND DO THEY UNDERSTAND THEIR EMERGENCY ROLES AND RESPONSIBILITIES?	INTERVIEW DATA CENTER STAFF.
	DO DATA CENTER STAFF RECEIVE PERIODIC TRAINING IN EMERGENCY FIRE, WATER, AND ALARM INCIDENT PROCEDURES?	REVIEW TRAINING RECORDS. REVIEW TRAINING COURSE DOCUMENTATION



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE EMERGENCY RESPONSE PROCEDURES DOCUMENTED?	REVIEW EMERGENCY RESPONSE PROCEDURES.
	ARE EMERGENCY PROCEDURES PERIODICALLY TESTED?	REVIEW TEST POLICIES.
5.2 ARCHIVING	HAS MANAGEMENT IMPLEMENTED A POLICY AND PROCEDURES FOR ENSURING THAT ARCHIVAL MEETS LEGAL AND BUSINESS REQUIREMENTS, AND IS PROPERLY SAFEGUARDED AND ACCOUNTED FOR?	REVIEW POLICIES AND PROCEDURES
5.3 CONTINUED INTEGRITY OF STORED DATA.	ARE THERE MANAGEMENT PROCEDURES TO ENSURE THAT THE INTEGRITY AND CORRECTNESS OF THE DATA KEPT ON FILES AND OTHER MEDIA (E.G., ELECTRONIC CARDS) IS CHECKED PERIODICALLY? SPECIFIC ATTENTION SHOULD BE PAID TO VALUE TOKENS, REFERENCE FILES AND FILES CONTAINING PRIVACY INFORMATION.	REVIEW PROCEDURES



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
5.4 RETENTION PERIODS AND STORAGE TERMS	ARE RETENTION PERIODS AND STORAGE TERMS DEFINED FOR DOCUMENTS, DATA, PROGRAMS AND REPORTS AND MESSAGES (INCOMING AND OUTGOING) AS WELL AS THE DATA (KEYS, CERTIFICATES) USED FOR THEIR ENCRYPTION AND AUTHENTICATION?	REVIEW PROCEDURES
5.5 MEDIA LIBRARY MANAGEMENT SYSTEM	ARE PROCEDURES ESTABLISHED TO ASSURE THAT CONTENTS OF ITS MEDIA LIBRARY CONTAINING DATA ARE INVENTORIED SYSTEMATICALLY, THAT ANY DISCREPANCIES DISCLOSED BY A PHYSICAL INVENTORY ARE REMEDIED IN A TIMELY FASHION AND THAT MEASURES ARE TAKEN TO MAINTAIN THE INTEGRITY OF MAGNETIC MEDIA STORED IN THE LIBRARY?	REVIEW PROCEDURES



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE STANDARDS DEFINED FOR THE EXTERNAL IDENTIFICATION OF MAGNETIC MEDIA AND THE CONTROL OF THEIR PHYSICAL MOVEMENT AND STORAGE TO SUPPORT ACCOUNTABILITY? RESPONSIBILITIES FOR MEDIA (MAGNETIC TAPE, CARTRIDGE, DISKS AND DISKETTES) LIBRARY MANAGEMENT SHOULD BE ASSIGNED TO SPECIFIC MEMBERS OF THE INFORMATION SERVICES FUNCTION.	REVIEW PROCEDURES AND EVIDENCE OF INVENTORY.
Back-up Management		
6.1 BACK-UP SITE AND HARDWARE.	DOES MANAGEMENT ENSURE THAT THE CONTINUITY METHODOLOGY INCORPORATES AN IDENTIFICATION OF ALTERNATIVES REGARDING THE BACK-UP SITE AND HARDWARE AS WELL AS A FINAL ALTERNATIVE SELECTION?	REVIEW BCP AND HOT SITE CONTRACT(S).



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	IS THE OFF-SITE STORAGE LOCATION GEOGRAPHICALLY REMOVED FROM THE PRIMARY SITE(S) AND PROTECTED BY ENVIRONMENTAL CONTROLS AND PHYSICAL ACCESS CONTROLS?	EXAMINE THE OFF-SITE STORAGE LOCATION.
	ARE SYSTEM AND APPLICATION DOCUMENTATION MAINTAINED AT THE OFF-SITE STORAGE LOCATION?	LOCATE AND EXAMINE DOCUMENTATION.
6.2 DATA AND PROGRAM BACK-UP PROCEDURES HAVE BEEN IMPLEMENTED.	ARE PROCEDURES IN PLACE FOR DATA STORAGE, WHICH CONSIDER RETRIEVAL REQUIREMENTS, AND COST EFFECTIVENESS AND SECURITY POLICY?	REVIEW PROCEDURES



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE BACKUP FILES CREATED ON A PRESCRIBED BASIS AND ROTATED OFF-SITE OFTEN ENOUGH TO AVOID DISRUPTION IF CURRENT FILES WERE LOST OR DAMAGED?	REVIEW WRITTEN POLICIES AND PROCEDURES FOR BACKING UP FILES. COMPARE INVENTORY RECORDS WITH THE FILES MAINTAINED OFF-SITE, AND DETERMINE THE AGE OF THESE FILES. FOR A SELECTION OF CRITICAL FILES, LOCATE AND EXAMINE THE BACKUP FILES. DETERMINE WHETHER BACKUP FILES ARE CREATED AND ROTATED OFF-SITE AS PRESCRIBED, AND ARE SENT BEFORE PRIOR VERSIONS ARE RETURNED.
	DO BACK-UP PROCEDURES FOR INFORMATION TECHNOLOGY-RELATED MEDIA INCLUDE THE PROPER STORAGE OF THE DATA FILES, SOFTWARE AND RELATED DOCUMENTATION, BOTH ON-SITE AND OFF-SITE?	REVIEW PROCEDURES



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	ARE BACK-UPS STORED SECURELY AND THE STORAGE SITES PERIODICALLY REVIEWED REGARDING PHYSICAL ACCESS SECURITY AND SECURITY OF DATA FILES AND OTHER ITEMS.	REVIEW PROCEDURES
6.3 BACK-UP AND RESTORATION	HAS MANAGEMENT IMPLEMENTED A PROPER STRATEGY FOR BACK UP AND RESTORATION TO ENSURE THAT IT INCLUDES A REVIEW OF BUSINESS REQUIREMENTS, AS WELL AS THE DEVELOPMENT, IMPLEMENTATION, TESTING AND DOCUMENTATION OF THE RECOVERY PLAN?	REVIEW PROCEDURES
6.4 BACK-UP JOBS	ARE PROCEDURES IN PLACE TO ENSURE BACK-UPS ARE TAKEN IN ACCORDANCE WITH THE DEFINED BACK-UP STRATEGY AND THE USABILITY OF BACK-UPS IS REGULARLY VERIFIED?	REVIEW PROCEDURES



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
Alternative Site Management		
7.1 ALTERNATIVE SITE IS MANAGED EFFECTIVELY.	DOES THE CONTINUITY METHODOLOGY ENSURE THAT THE USER DEPARTMENTS ESTABLISH ALTERNATIVE- PROCESSING PROCEDURES THAT MAY BE USED UNTIL THE INFORMATION SERVICES FUNCTION IS ABLE TO FULLY RESTORE ITS SERVICES AFTER A DISASTER OR EVENT?	REVIEW BCP
7.2 USER DEPARTMENT ALTERNATIVE PROCESSING	HAVE CONTRACTS OR INTERAGENCY AGREEMENTS BEEN ESTABLISHED FOR A BACK- UP DATA CENTER AND OTHER NEEDED FACILITIES THAT ARE IN A STATE OF READINESS COMMENSURATE WITH THE RISKS OF INTERRUPTED OPERATIONS, HAVE SUFFICIENT PROCESSING CAPACITY, AND ARE LIKELY TO BE AVAILABLE FOR USE?	REVIEW CONTRACTS AND AGREEMENTS.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
7.3 ALTERNATE DATA PROCESSING AND TELECOMMUNICATION FACILITIES	HAVE ALTERNATE TELECOMMUNICATION SERVICES BEEN ARRANGED?	REVIEW CONTRACTS AND AGREEMENTS.
	ARE ARRANGEMENTS PLANNED FOR TRAVEL AND LODGING OF NECESSARY PERSONNEL, IF NEEDED?	REVIEW BCP.
Interdependency Awareness		
8.1 ORGANIZATION IS AWARE OF INTERDEPENDENCIES.	HAS MANAGEMENT CONSIDERED THE EFFECT OF THE LOSS OF A NATIONAL INFRASTRUCTURE COMPONENT, SUCH AS: LOSS OF POWER FOR AN EXTENDED PERIOD OF TIME LOSS OF WATER SUPPLY LOSS OF TELECOMMUNICATIONS LOSS OF TRANSPORTATION SYSTEM LOSS OF OIL OR GAS	INTERVIEW SENIOR MANAGEMENT.



CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
8.2 MANAGEMENT HAS RECOGNIZED DEPENDENCE ON OUTSIDE SOURCES.	HAS THE ORGANIZATION CONSTRUCTED REDUNDANT RESOURCES IN CRITICAL AREAS?	INTERVIEW SENIOR MANAGEMENT. REVIEW ARCHITECTURE DIAGRAMS.
Monitoring		
9.1 MONITORING POLICIES AND PROCEDURES ARE IDENTIFIED.	HAS MANAGEMENT IMPLEMENTED A PROCESS TO ENSURE THAT THE PERFORMANCE OF INFORMATION TECHNOLOGY RESOURCES IS CONTINUOUSLY MONITORED AND EXCEPTIONS ARE REPORTED IN A TIMELY AND COMPREHENSIVE MANNER?	OBTAIN AND REVIEW NETWORK MONITORING REPORTS
9.2 MONITORING AND REPORTING	ARE PROBLEMS AND DELAYS ENCOUNTERED, THE REASON, AND THE ELAPSED TIME FOR RESOLUTION RECORDED AND ANALYZED TO IDENTIFY RECURRING PATTERNS OR TRENDS?	REVIEW “HELP DESK” RECORDS AND MANAGEMENT METRICS.
	ARE RECORDS MAINTAINED ON THE ACTUAL PERFORMANCE IN MEETING SERVICE SCHEDULES?	REVIEW MAINTENANCE RECORDS.



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
	DOES SENIOR MANAGEMENT PERIODICALLY REVIEW AND COMPARE THE SERVICE PERFORMANCE ACHIEVED WITH THE GOALS? DO THEY SURVEY USER DEPARTMENTS TO SEE IF THEIR NEEDS ARE BEING MET?	REVIEW TREND ANALYSIS REPORTS AND USER SURVEYS.
	IS USER SUPPORT ESTABLISHED WITHIN A “HELP DESK” FUNCTION?	REVIEW ORGANIZATIONAL STRUCTURE.
9.3 ASSIST AND ADVISE INFORMATION TECHNOLOGY CUSTOMERS	DO THE PROBLEM MANAGEMENT PROCEDURES CALL FOR ALL ISSUES TO BE LOGGED AND REPORTED THROUGH A SINGLE CONTROL POINT (I.E., THE PROBLEM MANAGEMENT SYSTEM) AND ASSIGNED THEIR OWN UNIQUE TRACKING NUMBER?	REVIEW TROUBLE TICKET REPORTS AND VERIFY THAT A UNIQUE INCIDENT NUMBER REFERS TO EACH INSTANCE. IF NO EVIDENCE IS AVAILABLE, RECORD AS AN EXCEPTION.
	ARE PROCEDURES IN PLACE TO ENSURE THAT ALL CUSTOMER QUERIES ARE ADEQUATELY REGISTERED BY THE “HELP DESK”?	IF YES, REVIEW TROUBLE TICKET REPORTS FOR EVIDENCE. IF NO, RECORD COMMENT AS EXCEPTION



CIAO

CONTINUITY OF SERVICES AND OPERATIONS

Control Objectives	Control Technique	Compliance Procedures
9.4 CUSTOMER QUERIES PROCESSES ARE ASSESSED.	DO “HELP DESK” PROCEDURES ENSURE THAT CUSTOMER QUERIES, WHICH CANNOT IMMEDIATELY BE RESOLVED, ARE APPROPRIATELY ESCALATED WITHIN THE INFORMATION SERVICES FUNCTION?	IF YES, REVIEW TROUBLE TICKET REPORTS FOR EVIDENCE. IF NO, RECORD COMMENT AS EXCEPTION.
	ARE THERE ESTABLISH PROCEDURES FOR TIMELY MONITORING OF THE CLEARANCE OF CUSTOMER QUERIES?	REVIEW TROUBLE TICKET REPORTS
	ARE LONG OUTSTANDING QUERIES INVESTIGATED AND ACTED UPON?	REVIEW TROUBLE TICKET REPORTS
	ARE PROCEDURES IN PLACE, WHICH ASSURE ADEQUATE REPORTING WITH REGARD TO CUSTOMER QUERIES AND RESOLUTION, RESPONSE TIMES AND TREND IDENTIFICATION? THE REPORTS SHOULD BE ADEQUATELY ANALYZED AND ACTED UPON.	IF YES, REVIEW PAST DATA AND SEE IF A TREND ANALYSIS HAS BEEN PERFORMED. IF NO, RECORD THE WEAKNESS



Appendix E: Change Control & Life Cycle Management

Control Objectives	Control Technique	Compliance Procedures
Change Management		
1.1 Authorizations for system modifications are documented and maintained	Are system change request forms used to document requests and related approvals?	Identify recent system modifications and determine whether change request forms were used. Examine a selection of system change request forms for approvals.
	Do both system users and data processing staff approve change requests?	Interview software development staff.
1.2 Changes are controlled through testing to final approval	Have test plan standards been developed for all levels of testing that define responsibilities for each party (e.g., users, system analysts, programmers, auditors, quality assurance, and library control)?	Review test plan standards.
	Are software changes documented so that they can be traced from code to design specifications and functional requirements?	Review test plan procedures. Review documentation.
	Are program changes moved into production only upon documented approval from user and system development management?	Review test plan procedures. Review documentation.
	Do data center management and/or the security administrators periodically review production program changes to determine whether access controls and change controls have been followed?	Interview data center management and security administrators.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
1.3 Emergency changes are promptly tested and approved	Are emergency change procedures documented?	Review procedures.
	Are emergency changes documented and <ul style="list-style-type: none">■ approved by the operations supervisor,■ formally reported to computer operations management for follow-up, and■ approved after the fact by programming supervisors and user management?	For a selection of emergency changes recorded in the emergency change log, review related documentation and approval.
1.4 Change Request Procedures Exist	Does management ensure that all requests for changes, system maintenance and supplier maintenance are standardized and are subject to formal change management procedures?	Interview senior management.
	Are changes categorized and prioritized, and are specific procedures in place to handle urgent matters?	Review change request procedures.
1.5 System Impact is Assessed	Is a procedure in place to ensure that all requests for change are assessed in a structured way for all possible impacts on the operational system and its functionality?	Review change control procedures.
1.6 Control of Changes is Managed	Does management ensure that change management, and software control and distribution are properly integrated with a comprehensive configuration management system?	Interview senior management.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
1.7 Documentation and Procedures are Updated	Does the change process ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly?	Review change control procedures. Review documentation.
1.8 Maintenance is Authorized	Does management ensure maintenance personnel have specific assignments and that their work is properly monitored?	Interview senior management.
	Does management ensure the system access rights of maintenance personnel are controlled to avoid risks of unauthorized access to automated systems?	Interview management. Review change control policies and procedures.
System Development Life Cycle Management		
2.1 A System Development Life Cycle Methodology has been implemented	Has a system development life cycle (SDLC) methodology been developed that provides a structured approach consistent with generally accepted concepts and practices?	Review SDLC methodology.
	Does it include active user involvement throughout the process?	Interview senior management. Interview active users.
	Is it sufficiently documented to provide guidance to staff with varying levels of skill and experience?	Review SDLC methodology documentation.
	Does it provide a means of controlling changes in requirements that occur over the system's life?	Review SDLC documentation.
	Does it include documentation requirements?	Review SDLC documentation.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
2.2 System Development Life Cycle Methodology is Updated	Does senior management implement a periodic review of its system development life cycle methodology to ensure that its provisions reflect current generally accepted techniques and procedures?	Interview senior management. Review SDLC documentation.
2.3 Coordination and Communication Processes Exist	Has management established a process for ensuring close coordination and communication between customers of the information services function and system implementers?	Interview senior management. Review communication and coordination process.
	Does this process entail structured methods using the system development life cycle methodology to ensure the provision of quality information technology solutions that meet the business demands?	Interview senior management. Interview system users.
	Does management promote an organization that is characterized by close cooperation and communication throughout the system development life cycle?	Interview senior management. Interview system users.
2.4 Program Documentation Standards Exist	Does the organization's system development life cycle methodology incorporate standards for program documentation that have been communicated to the concerned staff and enforced?	Review program documentation standards.
	Does the methodology ensure that the documentation created during information system development or modification projects conforms to these standards?	Review SDLC methodology. Review documentation.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
2.5 Methods for Design	Does the organization's system development life cycle methodology provide that appropriate procedures and techniques, involving close liaison with system users, are applied to create the design specifications for each new information system development project and to verify the design specifications against the user requirements?	Review SDLS methodology procedures and techniques. Review system design and verification process.
2.6 Source Data Collection Design	Does the organization's system development life cycle methodology require that adequate mechanisms for the collection and entry of data be specified for each information system development or modification project?	Review SDLC methodology.
2.7 Definition and Documentation for input/output Requirements	Does the organization's system development life cycle methodology require that adequate mechanisms exist for defining and documenting the input requirements for each information system development or modification project?	Review SDLC methodology.
2.8 Output Requirements Definition and Documentation	Does the organization's system development life cycle methodology require that adequate mechanisms exist for defining and documenting the output requirements for each information system development or modification project?	Review SDLC methodology.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
2.9 Interfaces are Defined	Does the organization's system development life cycle methodology provide that all external and internal interfaces are properly specified, designed and documented?	Review SDLC methodology.
	Does the organization's system development life cycle methodology provide for the development of an interface between the user and machine which is easy to use and self-documenting (by means of on-line help functions)?	Review SDLC methodology.
2.10 Requirements for Definition and Documentation Processing	Does the organization's system development life cycle methodology require that adequate mechanisms exist for defining and documenting the processing requirements for each information system development or modification project?	Review SDLC methodology.
2.11 Controllability is Assured	Does the organization's system development life cycle methodology require that adequate mechanisms for assuring the internal control and security requirements be specified for each information system development or modification project?	Review SDLC methodology.
	Does the methodology further ensure that information systems are designed to include application controls that guarantee the accuracy, completeness, timeliness and authorization of inputs, processing and outputs?	Review SDLC methodology.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
	Is a sensitivity assessment performed during initiation of system development or modification?	Interview senior management.
	Is the basic security and internal control aspects of a system to be developed or modified assessed along with the conceptual design of the system in order to integrate security concepts in the design as early as possible?	Review SDLC methodology. Interview senior management.
2.12 Availability is a Key Design Factor	Does the organization's system development life cycle methodology provide that availability is considered in the design process for new or modified information systems at the earliest possible stage?	Review SDLC methodology.
	Is availability analyzed and, if necessary, increased through maintainability and reliability improvements?	Interview senior management.
2.13 Conversion is Incorporated	Does the organization's system development life cycle methodology provide, as part of every information system development, implementation or modification project, that the necessary elements from the old system are converted to the new one according to a pre-established plan?	Review SDLC methodology.
2.14 Promotion to Production Process Exists	Does management define and implement formal procedures to control the handover of the system from development to testing to operations?	Interview senior management. Review handover control procedures.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
	Are the respective environments segregated and properly protected?	Interview senior management.
2.15 Evaluation of Meeting User Requirements is Conducted	Does organization's system development life cycle methodology require that a post-implementation review of operational information system requirements (e.g., capacity, throughput, etc.) be conducted to assess whether the users' needs are being achieved by the system?	Review SDLC methodology.
2.16 Post-Implementation Review is Conducted by Management	Does the organization's system development life cycle methodology require that a post-implementation review of an operational information system assess and report on whether the system delivered the benefits envisioned in the most cost effective manner?	Review SDLC methodology.
2.17 Disposal Process Exists	Does the system development life cycle methodology have procedures in place for disposal of systems and applications?	Review Disposal Procedures
Project Management		
3.1 Project Management Framework Exists	Has management established a general project management framework that defines the scope and boundaries of managing projects, as well as the project management methodology to be adopted and applied to each project undertaken?	Interview management. Review project management framework.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
	Does the methodology cover allocation of responsibilities, task breakdown, budgeting of time and resources, milestones, checkpoints and approvals?	Review project management methodology.
3.2 User Department Participates in Project Initiation	Does the organization's project management framework provide for participation by the affected user department management in the definition and authorization of a development implementation or modification project?	Review project management framework.
3.3 Project Team Membership and Responsibilities are Specified	Does the organization's project management framework specify the basis for assigning staff members to the project and define the responsibilities and authorities of the project team members?	Review project management framework.
3.4 Process exists for Project Definitions	Does the organization's project management framework provide for the creation of a clear written statement defining the nature and scope of every implementation project before work on the project begins?	Review project management framework.
3.5 Project is Approved	Does the organization's project management framework ensure that for each proposed project, the organization's senior management reviews the reports of the relevant feasibility studies as a basis for its decision on whether to proceed with the project?	Review project management framework. Interview senior management.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
3.6 Project Phases are Approved	Does the organization's project management frame-work provide for designated managers of the user and information services functions to approve the work accomplished in each phase of the cycle before work on the next phase begins?	Review project management framework.
3.7 Project Master Plan is Created	Does management ensure that for each approved project a project master plan is created which is adequate for maintaining control over the project throughout its life and which includes a method of monitoring the time and costs incurred throughout the life of the project.	Interview senior management. Review project master plans.
3.8 System Quality Assurance Plan Exists	Does management ensure that the implementation of a new or modified system includes the preparation of a quality plan that is then integrated with the project master plan and formally reviewed and agreed to by all parties concerned?	Interview senior management. Review quality plans.
3.9 Planning of Assurance Methods is Conducted	Are assurance tasks identified during the planning phase of the project management framework?	Review project management framework.
	Do assurance tasks support the accreditation of new or modified systems and assure that internal controls and security features meet the related requirements?	Review assurance tasks.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
3.10 Program for Formal Project Risk Management Exists	Has management implemented a formal project risk management program for eliminating or minimizing risks associated with individual projects?	Interview management. Review project risk management program.
3.11 Test Plan is Created	Does organization's project management framework require that a test plan be created for every development, implementation and modification project?	Review project management framework. Review test plans.
3.12 Post-Implementation Review Plan is Developed	Does the organization's project management framework provide for the development of a plan for a post-implementation review of every new or modified information system to ascertain whether the project has delivered the planned benefits?	Review project management framework. Review post-implementation review plans.
3.13 Design is Approved	Does the organization's system development life cycle methodology require that the design specifications for all information system development and modification projects be reviewed and approved by management, the affected user departments and the organization's senior management, when appropriate?	Review SDLC methodology. Review approval procedures.
3.14 File Requirements are Defined and Documented	Does the organization's system development life cycle methodology provide that an appropriate procedure be applied for defining and documenting the file format for each information system development or modification project?	Review SDLC methodology. Review file-type documentation procedures.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
3.15 Program Specifications are Prepared	Does the organization's system development life cycle methodology require that detailed written program specifications be prepared for each information system development or modification project?	Review SDLC methodology. Review program specification procedures.
	Does the methodology further ensure that program specifications agree with system design specifications?	Review SDLC methodology. Review program specification procedures.
3.16 System Design is Re-assessed	Does the organization's system development life cycle methodology ensure that the system design is re-assessed whenever significant technical and/or logical discrepancies occur during system development or maintenance?	Review SDLC methodology. Review program specification procedures.
3.17 Staff is Trained	Are staff of the affected user departments and the operations group of the information services function trained in accordance with the defined training plan and associated materials, as part of every information systems development, implementation or modification project.	Review training plan. Interview staff.
3.18 Application Software Performance Sizing is Established	Is application software performance sizing (optimization) established, as an integral part of the organization's system development life cycle methodology to forecast the resources required for operating new and significantly changed software?	Review SDLC methodology.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
Application Acquisition, Management, and Maintenance		
4.1 Software Release Policies Reviewed.	Does Management ensure that the release of software is governed by formal procedures ensuring sign-off, packaging, regression testing, handover, etc?	Review software release policies.
4.2 Distribution and implementation of new or revised software is controlled	Are standardized procedures used to distribute new software for implementation?	Examine procedures for distributing new software.
	Do internal control measures ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails?	Review internal control measures. Review audit trail documentation.
4.3 Use of public domain and personal software is restricted.	Are clear policies restricting the use of personal and public domain software developed and enforced?	Review pertinent policies and procedures Interview users and data processing staff.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
4.4 Programs are labeled and inventoried.	<p>Is library management software is used to:</p> <ul style="list-style-type: none">■ produce audit trails of program changes,■ maintain program version numbers,■ record and report program changes,■ maintain creation/date information for production modules,■ maintain copies of previous versions, and■ control concurrent updates?	<p>Review pertinent policies and procedures.</p> <p>Interview personnel responsible for library control.</p> <p>Determine how many prior versions of software modules are maintained.</p>
4.5 Access to Program Libraries is Restricted	<p>Are separate libraries maintained for program development and maintenance, testing, and production programs?</p>	<p>Examine libraries in use.</p> <p>Interview library control personnel.</p>
	<p>Is source code maintained in a separate library?</p>	<p>Examine libraries in use.</p>
	<p>Is access to all programs, including production code, source code, and extra program copies, protected by access control software and operating system features?</p>	<p>For critical software production programs, determine whether access control software rules are clearly defined.</p>
	<p>Are all deposits and withdrawals of tapes to the tape library authorized and logged?</p>	<p>Review deposit and withdrawal procedures.</p>



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
4.6 Movement of programs and data among libraries is controlled	Does a group independent of the user and programmers control movement of programs and data among libraries?	<p>Review pertinent policies and procedures.</p> <p>For a selection of program changes, examine related documentation to verify that</p> <ul style="list-style-type: none">■ procedures for authorizing movement among libraries were followed and■ before and after images were compared.
	Are before and after images of program code maintained and compared to ensure that only approved changes are made?	<p>Review pertinent policies and procedures.</p> <p>For a selection of program changes, examine related documentation to verify that</p> <ul style="list-style-type: none">■ procedures for authorizing movement among libraries were followed and■ before and after images were compared.
4.7 User Reference and Support Materials are prepared and updated	Are adequate user reference and support manuals prepared (preferably in electronic format) as part of every information system development or modification project?	<p>Review SDLC procedures.</p> <p>Review reference and support manuals.</p>
4.8 User Procedures Manuals are prepared and updated	Are adequate user procedure manuals prepared and refreshed as part of every information system development, implementation or modification project?	<p>Review SDLC procedures.</p> <p>Review procedure manuals.</p>



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
4.9 Operations Manual is adequate	Are adequate operations manuals prepared and kept up-to-date as part of every information system development, implementation or modification project?	Review SDLC procedures. Review operations manuals.
4.10 Training Materials are developed	Are adequate training materials developed as part of every information system development, implementation or modification project?	Review SDLC procedures. Review training materials.
Quality and Assurance		
5.1 General Quality Plan is maintained	Has senior management developed and regularly maintained an overall quality plan based on the organizational and information technology long-range plans?	Interview senior management. Review quality plan.
	Does the plan promote the continuous improvement philosophy and answer the basic questions of what, who and how?	Review quality plan.
5.2 Quality Assurance Approach is established	Has management established a standard approach regarding quality assurance that covers both general and project specific quality assurance activities?	Interview senior management. Review quality assurance approach.
	Does the approach prescribe the type(s) of quality assurance activities (such as reviews, audits, inspections, etc.) to be performed to achieve the objectives of the general quality plan?	Review quality assurance approach.
	Does the approach also require specific quality assurance reviews?	Review quality assurance approach.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
5.3 Quality Assurance Planning Process is implemented	Has management implemented a quality assurance planning process to determine the scope and timing of the quality assurance activities?	Interview senior management. Review quality assurance planning process.
5.4 Adherence to the Information Services Function's Standards and Procedures is reviewed	Does management ensure that the responsibilities assigned to the quality assurance personnel include a review of general adherence to the information services function's standards and procedures?	Interview senior management.
5.5 Adherence to Development Standards is evaluated	Does the organization's quality assurance approach require that a post-implementation review of an operational information system assess whether the project team adhered to the provisions of the system development life cycle methodology?	Review quality assurance approach.
5.6 The Quality Assurance Review of the Achievement of the Information Services Function's Objectives is reviewed	Does the quality assurance approach include a review of the extent to which particular systems and application development activities have achieved the objectives of the information services function?	Review quality assurance approach.
5.7 Quality Metrics are defined	Has management defined and used metrics to measure the results of activities, thus assessing whether quality goals have been achieved?	Interview senior management. Review metrics.
5.8 Reports of Quality Assurance Reviews are prepared	Are reports of quality assurance reviews prepared and submitted to management of user departments and the information services function?	Review quality assurance reviews.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
5.9 Program Testing Standards exist	Does the organization's system development life cycle methodology provide standards covering test requirements, verification, documentation and retention for testing individual software units and aggregated programs created as part of every information system development or modification project?	Review SDLC methodology.
5.10 Parallel/Pilot Testing is conducted	Does the organization's system development life cycle methodology define the circumstances under which parallel or pilot testing of new and/or existing systems will be conducted?	Review SDLC methodology.
5.11 System Testing is documented	Does the organization's system development life cycle methodology provide, as part of every information system development, implementation, or modification project, that the documented results of testing the system are retained?	Review SDLC methodology. Review testing documentation.
5.12 Information Technology Integrity Provisions in Application Program Software have been established	Has the organization established procedures to assure, where applicable, that application programs contain provisions which routinely verify the tasks performed by the software to help assure data integrity, and which provide in the restoration of the integrity through rollback or other means?	Review assurance procedures for integrity.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
5.13 Application Software Testing process is defined	Is unit testing, application testing, integration testing, system testing, and load and stress testing performed according to the project test plan and established testing standards before the user approves it?	Review project test plans. Review testing standards.
	Are adequate measures conducted to prevent disclosure of sensitive information used during testing?	Review controls for sensitive information.
	Have program staff and staff involved in developing and testing software been trained and are they familiar with the use of the organization's SDLC methodology?	Interview staff. Review training records.
	Are detailed system specifications prepared by the programmer and reviewed by a programming supervisor?	Interview staff.
	Are test plans documented and approved that define responsibilities for each party involved (e.g., users, systems analysts, programmers, auditors, quality assurance, library control)?	Review test plan documentation.
	Are unit, integration, and system testing performed and approved <ul style="list-style-type: none">■ in accordance with the test plan and■ applying a sufficient range of valid and invalid conditions?	Review testing procedures.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
	Is a comprehensive set of test transactions and data developed that represents the various activities and conditions that will be encountered in processing?	Review testing procedures.
	Are live data used in testing of program changes except to build test data files?	Review testing procedures.
5.14 Changes are Tested	Does management ensure that changes are tested in accordance with the impact and resource assessment in a separate test environment by an independent (from builders) test group before use in the regular operational environment begins?	Interview senior management. Review testing procedures.
	Are back-out plans developed?	Review back-out plans.
	Is acceptance testing carried out in an environment representative of the future operational environment?	Review testing procedures.
5.15 Parallel / Pilot Testing meets Criteria and Performance Standards	Are procedures in place to ensure that parallel or pilot testing is performed in accordance with a pre-established plan and that the criteria for terminating the testing process are specified in advance?	Review parallel and pilot procedures. Review test plans.
	Do procedures provide for a formal evaluation and approval of the test results by management of the affected user department(s) and the information services function?	Review testing procedures.



CHANGE CONTROL & LIFE CYCLE MANAGEMENT

Control Objectives	Control Technique	Compliance Procedures
5.16 Final Acceptance Test is adequate	Do the tests cover all components of the information system (e.g., application software, facilities, technology, and user procedures)?	Review testing procedures.
5.17 Security Testing and Accreditation Procedures are defined	Has management defined and implemented procedures to ensure that operations and user management formally accepts the test results and the level of security for the systems, along with the remaining residual risk?	Review acceptance procedures.
5.18 Operational Test Procedures Exist	Does management ensure that before moving the system into operation, the user or designated custodian validates its operation as a complete product, under conditions similar to the application environment and in the manner in which the system will be run in a production environment?	Interview senior management. Review testing procedures.

(Page Left Intentionally Blank)



CIAO

CHANGE CONTROL & LIFE CYCLE MANAGEMENT



Appendix F: System Software

Control Objectives	Control Technique	Compliance Procedures
System Software Access Control		
1.1 Access authorizations are appropriately limited.	Do policies and procedures exist for restricting access to systems software? If so, are they up-to-date?	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions. Observe personnel access system software. Attempt to access system software.
	Is access to system software restricted to a limited number of personnel, corresponding to job responsibilities? Are application programmers and computer operators specifically prohibited from accessing system software?	Review pertinent policies and procedures. Interview management and systems personnel regarding access restrictions.
	Is documentation showing justification and management approval for access to system software kept on file?	Select some systems programmers and determine whether management approved documentation supports their access to system software. Select some application programmers and determine whether they are not authorized access.
	Are access capabilities of system programmers periodically reviewed for propriety to see that access permissions correspond with job duties?	Determine the last time the access capabilities of system programmers were reviewed.



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
1.2 All access paths have been identified and controls implemented to prevent or detect access for all paths.	Is the operating system configured to prevent circumvention of the security software and application controls?	<p>Test the operating system parameters to verify that it is configured to maintain the integrity of the security software and application controls.</p> <p><i>The specifics of this step will be determined by the operating system in use. The auditor should consult audit guides for the operating system in use. This step may be facilitated by use of CA-EXAMINE, the DEC VAX Toolkit, or other audit tools. However, the auditor should be experienced in using the specific software tool, or seek the assistance of someone who is.</i></p>
		<p>Perform an operating system penetration analysis to determine if users can inappropriately utilize computer resources through direct or covert methods. Include the following:</p>
		<ul style="list-style-type: none">■ Determine whether the operating system's subsystems have been appropriately implemented to ensure that they support integrity controls.



CIAO

SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
		<ul style="list-style-type: none">■ Determine whether applications interfaces have been implemented to support operating system integrity controls, including: on-line transaction monitors, database software, on-line editors, on-line direct-access storage devices, on-line operating system datasets, exits related to the operating system, security, and program products, and controls over batch processing (including security controls, scheduler controls, and access authorities).
		<ul style="list-style-type: none">■ Evaluate the controls over external access to computer resources, including networks, dial-up, LAN, WAN, RJE, and the Internet.
		<ul style="list-style-type: none">■ Identify potential opportunities to adversely impact the operating system and its products through Trojan horses, viruses, and other malicious actions.



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
	Is access to system software restricted by access control software for personnel with appropriate job responsibilities? Is update access limited to primary and backup systems programmers? Are accesses to system software files logged by automated logging facilities?	Obtain a list of all system software on test and production libraries used by the entity. Verify that access control software restricts access to system software. Using security software reports, determine who has access to system software files, security software, and logging files. Reports should be generated in presence of auditor.
	Are vendor supplied default logon IDs and passwords disabled?	Inquire whether disabling has occurred. Test for their presence using vendor standard IDs and passwords.
	Is remote access to the system master console restricted? Do physical and logical controls provide security over all terminals that are set up as master consoles?	Determine what terminals are set up as master consoles and what controls exist over them.
System Software Monitoring (Access and Use)		
2.1 Policies and techniques have been implemented for using and monitoring use of system utilities.	Do policies and procedures for using and monitoring use of system software utilities exist? Are they up-to-date?	Review pertinent policies and procedures.
	Are responsibilities for using sensitive system utilities clearly defined? Do systems programmers understand their responsibilities?	Interview management and systems personnel regarding their responsibilities.



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
	Are responsibilities for monitoring use defined and understood by technical management?	Interview management and systems personnel regarding monitoring.
	Is the use of sensitive system utilities logged using access control software reports or job accounting data (e.g., IBM's System Management Facility)?	Determine whether logging occurs and what information is logged. Review logs. Using security software reports, determine who can access the logging files.
2.2 Inappropriate or unusual activity is investigated and appropriate actions taken.	Does technical management review the use of privileged system software and utilities?	Interview technical management regarding their reviews of privileged system software and utilities usage. Review documentation supporting their reviews.
	Is inappropriate or unusual activity in using utilities investigated?	Interview management and systems personnel regarding these investigations. Review documentation supporting these investigations.
	Are system programmers' activities monitored and reviewed?	Interview systems programmer supervisors to determine their activities related to supervising and monitoring their staff. Review documentation supporting their supervising and monitoring of systems programmers' activities



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
System Software Change Control		
3.1 System Software changes are authorized, tested, and approved before implementation.	Do up-to-date policies and procedures exist for identifying, selecting, installing, and modifying system software? Do procedures include an analysis of risks, costs and benefits, and consideration of the impact on processing reliability and security?	Review pertinent policies and procedures. Interview management and systems personnel.
	Do procedures exist for identifying and documenting system software problems? Do procedures include using a log to record the problem, the individual assigned to analyze the problem, and how the problem was resolved?	Review procedures for identifying and documenting system software problems. Interview management and systems programmers. Review the causes and frequency of any recurring system software problems, as recorded in the problem log, and ascertain if the change control process should have prevented these problems.
	Do new system software versions or products, and modifications to existing system software receive proper authorization? Are they supported by a change request document?	Determine what authorizations and documentation are required prior to initiating system software changes. Select recent system software changes and determine whether the authorization was obtained and the change is supported by a change request document.



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
	<p>Are new system software versions or products, and modifications to existing system software tested? Are the test results approved before implementation? Do procedures include:</p> <ul style="list-style-type: none">■ a written standard that guides the testing, which is conducted in a test rather than production environment;■ specification of the optional security related features to be turned on, when appropriate;■ review of test results by technically qualified staff, who document their opinion whether the system software is ready for production use; and■ review of test results and documented opinions by data center management prior to granting approval to move the system software into production use?	<p>Determine the procedures used to test and approve system software prior to its implementation.</p> <p>Select recent system software changes and test whether the indicated procedures were in fact used.</p>
	<p>Do procedures exist for controlling emergency changes? Do procedures include:</p> <ul style="list-style-type: none">■ authorizing and documenting emergency changes as they occur;■ reporting the change for management review; and■ review by an independent IS supervisor of the change.	<p>Review procedures used to control and approve emergency changes.</p> <p>Select some emergency changes to system software and test whether the indicated procedures were in fact used.</p>



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
3.2 Installation of system software is documented and reviewed.	Is installation of system software scheduled to minimize the impact on data processing, and is advance notice given to system users?	<p>Interview management and systems programmers about scheduling and giving advance notices when system software is installed.</p> <p>Review recent installations and determine whether scheduling and advance notification did occur.</p> <p>Determine whether better scheduling and notification of installations appears warranted to reduce impact on data processing operations.</p>
	Does an independent library control group perform migration of tested and approved system software to production use?	Interview management, systems programmers, and library control personnel, and determine who is responsible for the migration of approved system software to production libraries, and whether outdated versions are removed from production libraries.
	Are outdated versions of system software removed from production libraries?	Review supporting documentation for some system software migrations, and the removal of outdated versions from production libraries.
	Is installation of all system software logged to establish an audit trail and reviewed by data center management?	<p>Interview data center management about their role in reviewing system software installations.</p> <p>Review some recent system software installations and determine whether documentation shows that logging and management review occurred.</p>



SYSTEM SOFTWARE

Control Objectives	Control Technique	Compliance Procedures
	Is vendor supplied system software still supported by the vendor?	Interview system software personnel concerning a selection of system software and determine the extent to which the operating version of the system software is currently supported by the vendor.
	Is all system software current?	Interview management and systems programmers about the currency of system software and the currency and completeness of its documentation.
	Does current and complete documentation exist?	Review documentation and test whether recent changes are incorporated.
	Is a configuration baseline used as a checkpoint to return to after changes?	Review configuration baseline.
3.3 System Software maintenance is performed in accordance with system software change control procedures.	Do procedures exist for maintaining system software? Do procedures define the steps for making system software changes that result from maintenance activities?	Review procedures for maintaining system software. Interview management and systems personnel.
	Are third-party maintenance agreements in place? Do third-party maintenance agreements validate, protect, and maintain the software product's integrity rights while performing changes in accordance with system software change procedures?	Review third-party maintenance agreements.



CIAO

SYSTEM SOFTWARE

(Page Left Intentionally Blank)



CIAO

Appendix G: WHITE PAPER

*The Clinton Administration's Policy on Critical Infrastructure Protection:
Presidential Decision Directive 63
May 22, 1998*

This White Paper explains key elements of the Clinton Administration's policy on critical infrastructure protection. It is intended for dissemination to all interested parties in both the private and public sectors. It will also be used in U.S. Government professional education institutions, such as the National Defense University and the National Foreign Affairs Training Center, for coursework and exercises on interagency practices and procedures. Wide dissemination of this unclassified White Paper is encouraged by all agencies of the U.S. Government.

I. A Growing Potential Vulnerability

The United States possesses both the world's strongest military and its largest national economy. Those two aspects of our power are mutually reinforcing and dependent. They are also increasingly reliant upon certain critical infrastructures and upon cyber-based information systems.

Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. Many of the nation's critical infrastructures have historically been physically and logically separate systems that had little interdependence. As a result of advances in information technology and the necessity of improved efficiency, however, these infrastructures have become increasingly automated and interlinked. These same advances have created new vulnerabilities to equipment failures, human error, weather and other natural causes, and physical and cyber attacks. Addressing these vulnerabilities will necessarily require flexible, evolutionary approaches that span both the public and private sectors, and protect both domestic and international security.

Because of our military strength, future enemies, whether nations, groups or individuals, may seek to harm us in non-traditional ways including attacks within the United States. Our economy is increasingly reliant upon interdependent and cyber-supported infrastructures and non-traditional attacks on our infrastructure and information systems may be capable of significantly harming both our military power and our economy.



II. President's Intent

It has long been the policy of the United States to assure the continuity and viability of critical infrastructures. President Clinton intends that the United States will take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems.

III. A National Goal

No later than the year 2000, the United States shall have achieved an initial operating capability and no later than five years from the day the President signed Presidential Decision Directive 63 the United States shall have achieved and shall maintain the ability to protect our nation's critical infrastructures from intentional acts that would significantly diminish the abilities of:

- the Federal Government to perform essential national security missions and to ensure the general public health and safety;
- state and local governments to maintain order and to deliver minimum essential public services;
- the private sector to ensure the orderly functioning of the economy and the delivery of essential telecommunications, energy, financial and transportation services.

Any interruptions or manipulations of these critical functions must be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the United States.

IV. A Public-Private Partnership to Reduce Vulnerability

Since the targets of attacks on our critical infrastructure would likely include both facilities in the economy and those in the government, the elimination of our potential vulnerability requires a closely coordinated effort of both the public and the private sector. To succeed, this partnership must be genuine, mutual and cooperative. In seeking to meet our national goal to eliminate the vulnerabilities of our critical infrastructure, therefore, the U.S. government should, to the extent feasible, seek to avoid outcomes that increase government regulation or expand unfunded government mandates to the private sector.

For each of the major sectors of our economy that are vulnerable to infrastructure attack, the Federal Government will appoint from a designated Lead Agency a senior officer of that agency as the Sector Liaison Official to work with the private sector. Sector Liaison Officials, after discussions and coordination with private sector entities of their infrastructure sector, will identify a private sector counterpart (Sector Coordinator) to represent their sector.



CIAO

White Paper

Together these two individuals and the departments and corporations they represent shall contribute to a sectoral National Infrastructure Assurance Plan by:

- assessing the vulnerabilities of the sector to cyber or physical attacks;
- recommending a plan to eliminate significant vulnerabilities;
- proposing a system for identifying and preventing attempted major attacks;
- developing a plan for alerting, containing and rebuffing an attack in progress and then, in coordination with FEMA as appropriate, rapidly reconstituting minimum essential capabilities in the aftermath of an attack.

During the preparation of the sectoral plans, the National Coordinator (see section VI), in conjunction with the Lead Agency Sector Liaison Officials and a representative from the National Economic Council, shall ensure their overall coordination and the integration of the various sectoral plans, with a particular focus on interdependencies.

V. Guidelines

In addressing this potential vulnerability and the means of eliminating it, President Clinton wants those involved to be mindful of the following general principles and concerns.

- We shall consult with, and seek input from, the Congress on approaches and programs to meet the objectives set forth in this directive.
- The protection of our critical infrastructures is necessarily a shared responsibility and partnership between owners, operators and the government. Furthermore, the Federal Government shall encourage international cooperation to help manage this increasingly global problem.
- Frequent assessments shall be made of our critical infrastructures' existing reliability, vulnerability and threat environment because, as technology and the nature of the threats to our critical infrastructures will continue to change rapidly, so must our protective measures and responses be robustly adaptive.
- The incentives that the market provides are the first choice for addressing the problem of critical infrastructure protection; regulation will be used only in the face of a material failure of the market to protect the health, safety or well-being of the American people. In such cases, agencies shall identify and assess available alternatives to direct regulation, including providing economic incentives to encourage the desired behavior, or providing information upon which choices can be made by the private sector. These incentives, along with other actions, shall be designed to help harness the latest technologies, bring about global



CIAO

White Paper

solutions to international problems, and enable private sector owners and operators to achieve and maintain the maximum feasible security.

- The full authorities, capabilities and resources of the government, including law enforcement, regulation, foreign intelligence and defense preparedness shall be available, as appropriate, to ensure that critical infrastructure protection is achieved and maintained.
- Care must be taken to respect privacy rights. Consumers and operators must have confidence that information will be handled accurately, confidentially and reliably.
- The Federal Government shall, through its research, development and procurement, encourage the introduction of increasingly capable methods of infrastructure protection.
- The Federal Government shall serve as a model to the private sector on how infrastructure assurance is best achieved and shall, to the extent feasible, distribute the results of its endeavors.
- We must focus on preventative measures as well as threat and crisis management. To that end, private sector owners and operators should be encouraged to provide maximum feasible security for the infrastructures they control and to provide the government necessary information to assist them in that task. In order to engage the private sector fully, it is preferred that participation by owners and operators in a national infrastructure protection system be voluntary.
- Close cooperation and coordination with state and local governments and first responders is essential for a robust and flexible infrastructure protection program. All critical infrastructure protection plans and actions shall take into consideration the needs, activities and responsibilities of state and local governments and first responders.

VI. Structure and Organization

The Federal Government will be organized for the purposes of this endeavor around four components (elaborated in Annex A).

1. Lead Agencies for Sector Liaison: For each infrastructure sector that could be a target for significant cyber or physical attacks, there will be a single U.S. Government department which will serve as the lead agency for liaison. Each Lead Agency will designate one individual of Assistant Secretary rank or higher to be the Sector Liaison Official for that area and to cooperate with the private sector representatives (Sector Coordinators) in addressing problems related to critical infrastructure protection and, in particular, in recommending components of the National Infrastructure Assurance Plan. Together, the Lead Agency and the private sector counterparts will develop and implement a Vulnerability Awareness and Education Program for their sector.



CIAO

White Paper

2. Lead Agencies for Special Functions: There are, in addition, certain functions related to critical infrastructure protection that must be chiefly performed by the Federal Government (national defense, foreign affairs, intelligence, law enforcement). For each of those special functions, there shall be a Lead Agency which will be responsible for coordinating all of the activities of the United States Government in that area. Each lead agency will appoint a senior officer of Assistant Secretary rank or higher to serve as the Functional Coordinator for that function for the Federal Government.
3. Interagency Coordination: The Sector Liaison Officials and Functional Coordinators of the Lead Agencies, as well as representatives from other relevant departments and agencies, including the National Economic Council, will meet to coordinate the implementation of this directive under the auspices of a Critical Infrastructure Coordination Group (CICG), chaired by the National Coordinator for Security, Infrastructure Protection and Counter-Terrorism. The National Coordinator will be appointed by and report to the President through the Assistant to the President for National Security Affairs, who shall assure appropriate coordination with the Assistant to the President for Economic Affairs. Agency representatives to the CICG should be at a senior policy level (Assistant Secretary or higher). Where appropriate, the CICG will be assisted by extant policy structures, such as the Security Policy Board, Security Policy Forum and the National Security and Telecommunications and Information System Security Committee.
4. National Infrastructure Assurance Council: On the recommendation of the Lead Agencies, the National Economic Council and the National Coordinator, the President will appoint a panel of major infrastructure providers and state and local government officials to serve as the National Infrastructure Assurance Council. The President will appoint the Chairman. The National Coordinator will serve as the Council's Executive Director. The National Infrastructure Assurance Council will meet periodically to enhance the partnership of the public and private sectors in protecting our critical infrastructures and will provide reports to the President as appropriate. Senior Federal Government officials will participate in the meetings of the National Infrastructure Assurance Council as appropriate.

VII. Protecting Federal Government Critical Infrastructures

Every department and agency of the Federal Government shall be responsible for protecting its own critical infrastructure, especially its cyber-based systems. Every department and agency Chief Information Officer (CIO) shall be responsible for information assurance. Every department and agency shall appoint a Chief Infrastructure Assurance Officer (CIAO) who shall be responsible for the protection of all of the other aspects of that department's critical infrastructure. The CIO may be double-hatted as the CIAO at the discretion of the individual department. These officials shall establish procedures for obtaining expedient and valid authorizations to allow vulnerability assessments to be performed on government computer and physical systems. The Department of Justice shall establish legal guidelines for providing for such authorizations.



CIAO

White Paper

No later than 180 days from issuance of this directive, every department and agency shall develop a plan for protecting its own critical infrastructure, including but not limited to its cyber-based systems. The National Coordinator shall be responsible for coordinating analyses required by the departments and agencies of inter-governmental dependencies and the mitigation of those dependencies. The Critical Infrastructure Coordination Group (CICG) shall sponsor an expert review process for those plans. No later than two years from today, those plans shall have been implemented and shall be updated every two years. In meeting this schedule, the Federal Government shall present a model to the private sector on how best to protect critical infrastructure.

VIII. Tasks

Within 180 days, the Principals Committee should submit to the President a schedule for completion of a National Infrastructure Assurance Plan with milestones for accomplishing the following subordinate and related tasks.

1. Vulnerability Analyses: For each sector of the economy and each sector of the government that might be a target of infrastructure attack intended to significantly damage the United States, there shall be an initial vulnerability assessment, followed by periodic updates. As appropriate, these assessments shall also include the determination of the minimum essential infrastructure in each sector.
2. Remedial Plan: Based upon the vulnerability assessment, there shall be a recommended remedial plan. The plan shall identify timelines for implementation, responsibilities and funding.
3. Warning: A national center to warn of significant infrastructure attacks will be established immediately (see Annex A). As soon thereafter as possible, we will put in place an enhanced system for detecting and analyzing such attacks, with maximum possible participation of the private sector.
4. Response: A system for responding to a significant infrastructure attack while it is underway, with the goal of isolating and minimizing damage.
5. Reconstitution: For varying levels of successful infrastructure attacks, we shall have a system to reconstitute minimum required capabilities rapidly.



CIAO

White Paper

6. Education and Awareness: There shall be Vulnerability Awareness and Education Programs within both the government and the private sector to sensitize people regarding the importance of security and to train them in security standards, particularly regarding cyber systems.
7. Research and Development: Federally-sponsored research and development in support of infrastructure protection shall be coordinated, be subject to multi-year planning, take into account private sector research, and be adequately funded to minimize our vulnerabilities on a rapid but achievable timetable.
8. Intelligence: The Intelligence Community shall develop and implement a plan for enhancing collection and analysis of the foreign threat to our national infrastructure, to include but not be limited to the foreign cyber/information warfare threat.
9. International Cooperation: There shall be a plan to expand cooperation on critical infrastructure protection with like-minded and friendly nations, international organizations and multinational corporations.
10. Legislative and Budgetary Requirements: There shall be an evaluation of the executive branch's legislative authorities and budgetary priorities regarding critical infrastructure, and ameliorative recommendations shall be made to the President as necessary. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB.

The CICG shall also review and schedule the taskings listed in Annex B.

IX. Implementation

In addition to the 180-day report, the National Coordinator, working with the National Economic Council, shall provide an annual report on the implementation of this directive to the President and the heads of departments and agencies, through the Assistant to the President for National Security Affairs. The report should include an updated threat assessment, a status report on achieving the milestones identified for the National Plan and additional policy, legislative and budgetary recommendations. The evaluations and recommendations, if any, shall be coordinated with the Director of OMB. In addition, following the establishment of an initial operating capability in the year 2000, the National Coordinator shall conduct a zero-based review.



Annex A: Structure and Organization

Lead Agencies: Clear accountability within the U.S. Government must be designated for specific sectors and functions. The following assignments of responsibility will apply.

Lead Agencies for Sector Liaison:

Commerce	Information and communications
Treasury	Banking and finance
EPA	Water supply
Transportation	Aviation Highways (including trucking and intelligent transportation systems) Mass transit Pipelines Rail Waterborne commerce
Justice/FBI	Emergency law enforcement services
FEMA	Emergency fire service Continuity of government services
HHS	Public health services, including prevention, surveillance, laboratory services and personal health services
Energy	Electric power Oil and gas production and storage

Lead Agencies for Special Functions:

Justice/FBI	Law enforcement and internal security
CIA	Foreign intelligence
State	Foreign affairs
Defense	National defense



CIAO

White Paper

In addition, OSTP shall be responsible for coordinating research and development agendas and programs for the government through the National Science and Technology Council. Furthermore, while Commerce is the lead agency for information and communication, the Department of Defense will retain its Executive Agent responsibilities for the National Communications System and support of the President's National Security Telecommunications Advisory Committee.

National Coordinator: The National Coordinator for Security, Infrastructure Protection and Counter-Terrorism shall be responsible for coordinating the implementation of this directive. The National Coordinator will report to the President through the Assistant to the President for National Security Affairs. The National Coordinator will also participate as a full member of Deputies or Principals Committee meetings when they meet to consider infrastructure issues. Although the National Coordinator will not direct Departments and Agencies, he or she will ensure interagency coordination for policy development and implementation, and will review crisis activities concerning infrastructure events with significant foreign involvement. The National Coordinator will provide advice, in the context of the established annual budget process, regarding agency budgets for critical infrastructure protection. The National Coordinator will chair the Critical Infrastructure Coordination Group (CICG), reporting to the Deputies Committee (or, at the call of its chair, the Principals Committee). The Sector Liaison Officials and Special Function Coordinators shall attend the CICG's meetings. Departments and agencies shall each appoint to the CICG a senior official (Assistant Secretary level or higher) who will regularly attend its meetings. The National Security Advisor shall appoint a Senior Director for Infrastructure Protection on the NSC staff.

A National Plan coordination (the Critical Infrastructure Assurance Office -- CIAO) staff will be contributed on a non-reimbursable basis by the departments and agencies, consistent with law. The CIAO staff will integrate the various sector plans into a National Infrastructure Assurance Plan and coordinate analyses of the U.S. Government's own dependencies on critical infrastructures. The CIAO staff will also help coordinate a national education and awareness program, and legislative and public affairs.

The Defense Department shall continue to serve as Executive Agent for the Commission Transition Office, which will form the basis of the CIAO, during the remainder of FY98. Beginning in FY99, the CIAO shall be an office of the Commerce Department. The Office of Personnel Management shall provide the necessary assistance in facilitating the CIAO's operations. The CIAO will terminate at the end of FY01, unless extended by Presidential directive.

Warning and Information Centers

As part of a national warning and information sharing system, the President immediately authorizes the FBI to expand its current organization to a full scale National Infrastructure Protection Center (NIPC). This organization shall serve as a national critical infrastructure threat assessment, warning, vulnerability, and law enforcement investigation and response entity. During the initial period of six to twelve months, the President also directs the National Coordinator and the Sector Liaison



CIAO

White Paper

Officials, working together with the Sector Coordinators, the Special Function Coordinators and representatives from the National Economic Council, as appropriate, to consult with owners and operators of the critical infrastructures to encourage the creation of a private sector sharing and analysis center, as described below.

National Infrastructure Protection Center (NIPC): The NIPC will include FBI, USSS, and other investigators experienced in computer crimes and infrastructure protection, as well as representatives detailed from the Department of Defense, the Intelligence Community and Lead Agencies. It will be linked electronically to the rest of the Federal Government, including other warning and operations centers, as well as any private sector sharing and analysis centers. Its mission will include providing timely warnings of intentional threats, comprehensive analyses and law enforcement investigation and response.

All executive departments and agencies shall cooperate with the NIPC and provide such assistance, information and advice that the NIPC may request, to the extent permitted by law. All executive departments shall also share with the NIPC information about threats and warning of attacks and about actual attacks on critical government and private sector infrastructures, to the extent permitted by law. The NIPC will include elements responsible for warning, analysis, computer investigation, coordinating emergency response, training, outreach and development and application of technical tools. In addition, it will establish its own relations directly with others in the private sector and with any information sharing and analysis entity that the private sector may create, such as the Information Sharing and Analysis Center described below.

The NIPC, in conjunction with the information originating agency, will sanitize law enforcement and intelligence information for inclusion into analyses and reports that it will provide, in appropriate form, to relevant federal, state and local agencies; the relevant owners and operators of critical infrastructures; and to any private sector information sharing and analysis entity. Before disseminating national security or other information that originated from the intelligence community, the NIPC will coordinate fully with the intelligence community through existing procedures. Whether as sanitized or unsanitized reports, the NIPC will issue attack warnings or alerts to increases in threat condition to any private sector information sharing and analysis entity and to the owners and operators. These warnings may also include guidance regarding additional protection measures to be taken by owners and operators. Except in extreme emergencies, the NIPC shall coordinate with the National Coordinator before issuing public warnings of imminent attacks by international terrorists, foreign states or other malevolent foreign powers.

The NIPC will provide a national focal point for gathering information on threats to the infrastructures. Additionally, the NIPC will provide the principal means of facilitating and coordinating the Federal Government's response to an incident, mitigating attacks, investigating threats and monitoring reconstitution efforts. Depending on the nature and level of a foreign threat/attack, protocols established between special function agencies (DOJ/DOD/CIA), and the ultimate decision of the President, the NIPC may be placed in a direct support role to either DOD or the Intelligence Community.



CIAO

White Paper

Information Sharing and Analysis Center (ISAC): The National Coordinator, working with Sector Coordinators, Sector Liaison Officials and the National Economic Council, shall consult with owners and operators of the critical infrastructures to strongly encourage the creation of a private sector information sharing and analysis center. The actual design and functions of the center and its relation to the NIPC will be determined by the private sector, in consultation with and with assistance from the Federal Government. Within 180 days of this directive, the National Coordinator, with the assistance of the CICG including the National Economic Council, shall identify possible methods of providing federal assistance to facilitate the startup of an ISAC.

Such a center could serve as the mechanism for gathering, analyzing, appropriately sanitizing and disseminating private sector information to both industry and the NIPC. The center could also gather, analyze and disseminate information from the NIPC for further distribution to the private sector. While crucial to a successful government-industry partnership, this mechanism for sharing important information about vulnerabilities, threats, intrusions and anomalies is not to interfere with direct information exchanges between companies and the government.

As ultimately designed by private sector representatives, the ISAC may emulate particular aspects of such institutions as the Centers for Disease Control and Prevention that have proved highly effective, particularly its extensive interchanges with the private and non-federal sectors. Under such a model, the ISAC would possess a large degree of technical focus and expertise and non-regulatory and non-law enforcement missions. It would establish baseline statistics and patterns on the various infrastructures, become a clearinghouse for information within and among the various sectors, and provide a library for historical data to be used by the private sector and, as deemed appropriate by the ISAC, by the government. Critical to the success of such an institution would be its timeliness, accessibility, coordination, flexibility, utility and acceptability.



Annex B: Additional Taskings

Studies

The National Coordinator shall commission studies on the following subjects:

- Liability issues arising from participation by private sector companies in the information sharing process.
- Existing legal impediments to information sharing, with an eye to proposals to remove these impediments, including through the drafting of model codes in cooperation with the American Legal Institute.
- The necessity of document and information classification and the impact of such classification on useful dissemination, as well as the methods and information systems by which threat and vulnerability information can be shared securely while avoiding disclosure or unacceptable risk of disclosure to those who will misuse it.
- The improved protection, including secure dissemination and information handling systems, of industry trade secrets and other confidential business data, law enforcement information and evidentiary material, classified national security information, unclassified material disclosing vulnerabilities of privately owned infrastructures and apparently innocuous information that, in the aggregate, it is unwise to disclose.
- The implications of sharing information with foreign entities where such sharing is deemed necessary to the security of United States infrastructures.
- The potential benefit to security standards of mandating, subsidizing, or otherwise assisting in the provision of insurance for selected critical infrastructure providers and requiring insurance tie-ins for foreign critical infrastructure providers hoping to do business with the United States.



Public Outreach

In order to foster a climate of enhanced public sensitivity to the problem of infrastructure protection, the following actions shall be taken:

- The White House, under the oversight of the National Coordinator, together with the relevant Cabinet agencies shall consider a series of conferences: (1) that will bring together national leaders in the public and private sectors to propose programs to increase the commitment to information security; (2) that convoke academic leaders from engineering, computer science, business and law schools to review the status of education in information security and will identify changes in the curricula and resources necessary to meet the national demand for professionals in this field; (3) on the issues around computer ethics as these relate to the K through 12 and general university populations.
- The National Academy of Sciences and the National Academy of Engineering shall consider a round table bringing together federal, state and local officials with industry and academic leaders to develop national strategies for enhancing infrastructure security.
- The intelligence community and law enforcement shall expand existing programs for briefing infrastructure owners and operators and senior government officials.
- The National Coordinator shall (1) establish a program for infrastructure assurance simulations involving senior public and private officials, the reports of which might be distributed as part of an awareness campaign; and (2) in coordination with the private sector, launch a continuing national awareness campaign, emphasizing improving infrastructure security.

Internal Federal Government Actions

In order for the Federal Government to improve its infrastructure security, these immediate steps shall be taken:

- The Department of Commerce, the General Services Administration, and the Department of Defense shall assist federal agencies in the implementation of best practices for information assurance within their individual agencies.
- The National Coordinator shall coordinate a review of existing federal, state and local bodies charged with information assurance tasks, and provide recommendations on how these institutions can cooperate most effectively.
- All federal agencies shall make clear designations regarding who may authorize access to their computer systems.



CIAO

White Paper

- The Intelligence Community shall elevate and formalize the priority for enhanced collection and analysis of information on the foreign cyber/information warfare threat to our critical infrastructure.
- The Federal Bureau of Investigation, the Secret Service and other appropriate agencies shall: (1) vigorously recruit undergraduate and graduate students with the relevant computer-related technical skills for full-time employment as well as for part-time work with regional computer crime squads; and (2) facilitate the hiring and retention of qualified personnel for technical analysis and investigation involving cyber attacks.
- The Department of Transportation, in consultation with the Department of Defense, shall undertake a thorough evaluation of the vulnerability of the national transportation infrastructure that relies on the Global Positioning System. This evaluation shall include sponsoring an independent, integrated assessment of risks to civilian users of GPS-based systems, with a view to basing decisions on the ultimate architecture of the modernized NAS on these evaluations.
- The Federal Aviation Administration shall develop and implement a comprehensive National Airspace System Security Program to protect the modernized NAS from information-based and other disruptions and attacks.
- GSA shall identify large procurements (such as the new Federal Telecommunications System, FTS 2000) related to infrastructure assurance, study whether the procurement process reflects the importance of infrastructure protection and propose, if necessary, revisions to the overall procurement process to do so.
- OMB shall direct federal agencies to include assigned infrastructure assurance functions within their Government Performance and Results Act strategic planning and performance measurement framework.
- The NSA, in accordance with its National Manager responsibilities in NSD-42, shall provide assessments encompassing examinations of U.S. Government systems to interception and exploitation; disseminate threat and vulnerability information; establish standards; conduct research and development; and conduct issue security product evaluations.



CIAO

White Paper

Assisting the Private Sector

In order to assist the private sector in achieving and maintaining infrastructure security:

- The National Coordinator and the National Infrastructure Assurance Council shall propose and develop ways to encourage private industry to perform periodic risk assessments of critical processes, including information and telecommunications systems.
- The Department of Commerce and the Department of Defense shall work together, in coordination with the private sector, to offer their expertise to private owners and operators of critical infrastructure to develop security-related best practice standards.
- The Department of Justice and Department of the Treasury shall sponsor a comprehensive study compiling demographics of computer crime, comparing state approaches to computer crime and developing ways of deterring and responding to computer crime by juveniles.



CIAO

White Paper

(Page Left Intentionally Blank)

Produced by:

**KPMG Peat Marwick LLP
2001 M Street, N.W.
Washington, D.C. 20036-3389
Telephone: 202-530-6441**